Vital Interests, Virtual Threats

Reconciling International Law with Information Warfare and United States Security

Karl J. Shawhan, Major, USAF
School of Advanced Airpower Studies

THESIS PRESENTED TO THE FACULTY OF
THE SCHOOL OF ADVANCED AIRPOWER STUDIES,
MAXWELL AIR FORCE BASE, ALABAMA, FOR COMPLETION OF
GRADUATION REQUIREMENTS, ACADEMIC YEAR 1998–99.

Air University Press
Maxwell Air Force Base, Alabama

March 2001

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of Air University, the United States Air Force, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

Contents

Chapter *Page*

Illustrations

Figure

Figure *Page*

Table

Abstract

The dominance of the United States (US) military means that traditional threats, short of weapons of mass destruction, currently pose little risk to US sovereignty. Nontraditional threats, however, pose asymmetric dilemmas for the United States. The increased US military and economic reliance on information systems introduces new vulnerabilities not adequately protected by traditional kinetic force arms. Additionally, international law does not adequately provide response mechanisms for the United States in case of a computer network attack. The United States needs to establish policy directives and diplomatic initiatives to secure its information sovereignty for the future.

This study examines the history of technology and sovereignty, which reveals a model for the evolution of international law. Specifically, the history of sea, air, and space provides examples on past issues of sovereignty. A three-stage pattern of international law emerges. Under the assumption that sovereignty issues related to information warfare will follow the same path, the current state of sovereignty regarding information is established. To focus the study, a functional outline for international convention, the International Regime for Information Security (IRIS), is advanced. IRIS balances US domestic privacy needs with US national security demands. Specifically, technology issues regarding digital identification and encryption are weighed against civil liberties and intelligence needs.

After examining the advantages and disadvantages of the IRIS regime, this study recommends its use as a model for a future international convention on information warfare. Within an IRIS-type regime, compromise between civil liberty advocates and intelligence service organizations are necessary. Through digital identification and universally strong encryption, privacy and security concerns will be satisfied.

About the Author

Maj Karl J. Shawhan (BSCSE, Northern Arizona University [NAU]; MAS, Embry–Riddle Aeronautical University) is a senior pilot with more than 2,000 flying hours. He was commissioned through the Reserve Officer Training Corps at NAU in 1986. Graduating from undergraduate navigator training in 1987, Major Shawhan went on to fly B-52s at K. I. Sawyer Air Force Base (AFB), Michigan, as a navigator, progressing to become an evaluator navigator. Selected for pilot training, he graduated from undergraduate pilot training at Laughlin AFB, Texas, in 1991. He completed initial qualification training in the B-1B bomber at Dyess AFB, Texas, in 1992 and remained there to fly as a copilot, aircraft commander, and instructor pilot. Major Shawhan is a graduate of the Command and General Staff College at Fort Leavenworth, Kansas, and the School of Advanced Airpower Studies. In July 1998, Major Shawhan was assigned to US Atlantic Command, J9 (Joint Experimentation), Concepts Division, as the branch chief for Experimentation and Analysis.

Acknowledgments

First, I thank my wife, Amber, and our five children—Andy, Caroline, Peter, Timothy, and Nicholas—for their sacrifices. Second, I also recognize faculty mentors Dr. Karl P. Mueller and Lt Col David L. Coulliette for their guidance in my thesis preparation. Third, I thank Col Stephen E. Wright, 1993 School of Advanced Airpower Studies graduate, for his encouragement and support.

Chapter 1

Introduction

One very important reason for disliking a weapon was, of course, because it was new. A weapon might or might not be effective, but whenever one was introduced it always threatened to upset traditional ideas as to how war should be waged, and, indeed, what it was all about.

—Martin L. van Creveld
The Transformation of War

Revolutions in the human environment have frequently caused radical visions of the future. Giulio Douhet spun the advent of airpower into cataclysmic battles for *Command of the Air;* nuclear weapons were forecast to bring an end to war—or the world; sputnik was a harbinger of future Soviet domination; acquired immune deficiency syndrome (AIDS) or the Ebola virus was certain to devastate mankind as the medieval Black Death had decimated Europe. In the United States (US), the revolution of computer network technology has encouraged notions of computer domination in a bloodless conflict or an apocalyptic reckoning with the year 2000 (Y2K). As with previous revolutions, the aftermath of computer ascendance will lie somewhere short of extreme imagination.

In hindsight the hyperbole accompanying past revolutions acted as an engine for policy debate. Airpower advocates clung to Douhet in their call for a separate service and for bomber-friendly budgets. The cold war started with a petition for United Nations (UN) control over a world nuclear arsenal and, instead, resulted in a costly nuclear arms race. Space provided a peaceful outlet for cold war competition in a race to put a man on the moon. If there is a computer revolution, it is imperative that policy guidance be based upon a realistic view of the likely outcome.

Purpose of this Study

The United States currently enjoys the status of sole world superpower. With benevolence being in the eye of the beholder, it is possible to imagine adversarial threats emerging. The dominance of the US military indicates that traditional threats, short of weapons of mass destruction (WMD), pose no present risk to US sovereignty. As the world's economic leader, the United States is ahead in the transition to a knowledge-based economy. The United States has leveraged its information dominance to produce a robust information warfare (IW) capability. However, the new economy brings with it new vulnerabilities that may not be adequately protected by conventional weapons or modern information arms. With the buy-in cost for IW capability extremely low, a knowledgeable cyberenemy can mass an attack along many axes simultaneously. The United States needs to secure its exposed positions through protection, deterrence, and—if necessary—response. Lacking a symmetric adversary, a proportionate cyberresponse may be unavailable.

This study discusses how the use of computer networks threatens the traditional understanding of national sovereignty. It attempts to determine whether the United States can deter or adequately respond to computer-based threats while remaining within the existing international legal regime. The conclusion rests upon the foundation of international law regarding war and an analysis of sovereignty as applied in the realms of sea, air, and outer space. It examines how far advances in technology have outpaced the intent of the Charter of the UN regarding aggression and armed force. After proving the existence of a computer revolution, this study examines the extremes in current rhetoric. Finally, this study proposes reasonable policy steps necessary to support national security in an information age. It determines the advantage that might be gained through a change in international law defining where information operations (IO) cross from peaceful action to aggressive action to armed force. In doing so, this study balances the security that certainty and openness provide against the flexibility that ambiguity affords.

War and Morality

While theologians can point to references in the Bible that illustrate morality and righteousness in war, Saint Thomas Aquinas was the first to apply the Scholastic method in a study of virtue in war.[1] In his theological work, *Summa Theologica* (1266–73), he explored two areas of war:

Jus ad bellum—the right to go to war (conflict management); and
Jus in bello—the right conduct during war (rules of hostilities).

Subsequently, his work became the model for *The Law of War and Peace*, by Hugo Grotius (1583–1645), considered by many to be the father of international law.[2] While the use of information attack during war is important, classification requirements will limit this study principally to the issue of *jus ad bellum*.

Lacking a divine mandate to conduct war, the paradox of a just war construct is that some nation must break the rules to start a war. Authors in the Middle Ages received encouragement from the Catholic Church to define a *jus ad bellum* (just war)—to describe those affairs in which Christians could fight with clear conscience. Five principles, which still apply today, emerged.

- War must be waged by a legitimate authority.
- The cause must be just reparation for injury or to restore what had been wrongly seized.
- It must have the intention of advancing good or avoiding evil.

- There must be a reasonable prospect of victory.
- Every effort must be made to reconcile differences by peaceful means.[3]

After World War I, "the war to end all wars," efforts were made to strengthen international law to prevent war. Specifically, President Woodrow Wilson's League of Nations was an effort at collective security—not through force, but through peaceful interdependence. Wilson remarked, "If any Member of the League breaks or ignores these promises with regard to arbitration and discussions, what happens, War? No, not War but something more tremendous than war. Apply this economic, peaceful, silent, deadly remedy and there will be no need for force. The boycott is what is substituted for war. A nation that is boycotted is a nation that is in sight of surrender."[4] In the 1920s under the threat of League boycott, Yugoslavia removed troops from Albania; and Greece renounced territorial claims on Bulgarian territory.[5] But confidence in state "peer pressure" achieving peaceful resolutions ended with Italy's attack against Ethiopia in October 1935. Mindful of the balance of power emerging with a resurgent Nazi Germany, Britain and France were reluctant to excoriate Fascist Italy. Britain and France eliminated oil restrictions, and sanctions failed to cause a reversal. When Italy's intransigence became apparent, the League revoked the sanctions in a futile effort to avoid sending Benito Mussolini into Adolf Hitler's camp.[6]

Recent US policy, such as the Weinberger Doctrine, reflects these principles to internationally legitimize the employment of armed force. When possible the United States achieves legitimacy through approval of the UN. As the League of Nations before it, the UN attempts to prevent conflict by establishing strict requirements for just war in a collective response while condemning unjust war.

The UN on Just War

The Charter of the UN establishes guidelines for the legitimate use of armed force. More importantly, it mandates peaceful resolution of disputes. Article 2 spells out the pacific nature of the charter with regards to international relations. Based on the principle of "sovereign equality," the charter demands peaceful settlement of disputes while proscribing the threat or use of force against another member.[7] Like the League of Nations before it, the UN includes means for settling differences of opinion.

Conflict Resolution

Chapter VI, "Pacific Settlement of Disputes," mandates pacific methods to settle disputes. Specifically, it orders members to "first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice."[8] Lacking a satisfactory resolution, the potential belligerents are to submit to the Security Council's mediation. Chapter VII, "Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression," describes the Security Council's role in conflict arbitration. Barring a resolution, the Security Council can invoke measures not involving the use of armed force to encourage compliance. "These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."[9] Ultimately, the Security Council may consider a "blockade, and other operations by air, sea, or land forces of Members of the United Nations."

Naturally, member states are reluctant for the UN to label them as aggressors. However, within the context of most disputes (as with children), it is difficult to determine who committed the first offense. Due to the prevalence of the term *aggression* in the UN charter, the General Assembly clarified its meaning in a 1974 resolution. The resolution enumerates several explicit means of aggression to include invasion or armed attack, bombardment, blockade, the use of forces located in another state, and the sending of armed bands or mercenaries.[10] It clarifies those acts to be avoided in fear of collective UN response. In recognizing changes in the means of warfare, the resolution qualifies that, "The acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter."[11] In matters of explicit aggression, a victim state is not required to turn the other cheek while the Security Council debates.

Self-Defense

During negotiations in San Francisco, California, in 1945, the United States required clarification on the legitimacy of regional collective security arrangements. Specifically, US adherence to the Monroe Doctrine and the right of national self-defense required an acknowledgment of supplementary security rights.[12] In an effort to quell anxiety about the timeliness of Security Council attention, Chapter VII included a loophole for responding without resorting to Security Council adjudication. Article 51 allows,

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[13]

This exception stipulates that the only type of aggression permitting a nonbrokered response is one of armed attack. Article 51 "left ambiguous the precise boundary between enforcement action by the Security Council and actions that might permissibly be taken in self-defense."[14] In matters of unarmed conflict, this ambiguity could represent a veil for flexible response or a gap in a security framework.

During a dispute the Security Council's ability to decide what constitutes an act of aggression allows for a collective response in unforeseen circumstances. If a state can afford to wait for Security Council judgment, this is an appropriate means for establishing precedent. Urgent matters, however, may require unilateral action. In situations not involving the use of classic armed force, the mandate for restraint may be too much to ask. For this reason the definitions of aggression and armed attack may need to be revised to acknowledge a new paradigm.

An Information Revolution

Several advances preceded the current revolution in information technology.[15] In the mid-1800s, the telegraph and railroad heralded a revolution in communication. By 1866 telegraph cables linked the United States and Europe while networks developed on both continents. In 1876 the telephone increased the ability to communicate by an order of magnitude and left telegraph operators with new jobs at switchboards. The advent of wireless radio early this century offered new opportunities to provide mass communication. In the middle of the twentieth century, the advances of television and satellite communication greatly increased the amount of timely information communicated through a single medium. Each of these technological advances led to social, economic, political, and military changes.[16] Daniel S. Papp, David S. Alberts, and Alexander J. Tuyahov have posited that the Soviet society, which attempted to limit free communication, could not adapt to emerging information technologies and collapsed in its competition with the West.[17] Since the end of the cold war, communication throughput has increased by yet another order of magnitude.

The information age is redefining the ways to measure wealth and status. Previously, natural resources and physical labor were broad measurements of the wealth of a business, a corporation, or a state.[18] With the globalization of markets and the spread of information technology and computer networks, knowledge and communication are becoming the modern barometer for ascendancy and are changing the face of the workforce.

During the Industrial Revolution, mechanization displaced the vast agricultural labor pool. These workers were welcomed into the new urban regions where manufacturing work was labor-intensive. Presently, while trade protectionists lament the loss of jobs to cheap overseas labor markets, the US labor pool is converting to a service- or knowledge-based workforce. International Business Machines (IBM) has reduced its 1985 workforce of 406,000 by two-thirds. Volkswagen intends to reduce its present workforce by one-third. Proctor and Gamble has rising sales, yet is dismissing 12 percent of its workforce.[19] The hyperinflation in the price of Internet stocks demonstrates the belief that the marketplace as we know it is in the midst of a profound revolution. “Rent in cyberspace is even cheaper than catalogue space, and much lower than rent at the mall.”[20] Where 2 percent of the workforce now feeds an entire nation, how might the job market appear when 2 percent manufacture all goods, and another 2 percent arrange for the marketing and delivery? Future society will have drastically different demographics than the present. Administration based upon outdated paradigms will poorly serve national security interests. What type of dependencies or vulnerabilities will an information age herald?

Overview of this Study

This study determines if the existing colloquium of international law adequately addresses the needs of the United States concerning computer network attack (CNA). Chapter 2 provides a historical review of the development of international law regarding sovereignty in the realms of sea, air, and outer space. Chapter 3 describes the expanding importance, and attendant vulnerabilities, of information to society. Chapter 4 examines how existing international law concerning national sovereignty applies to IW. Chapter 5 describes a possible international regime protecting national information sovereignty. Chapter 6 reviews the advantages and risks of such a regime.

Assumptions and Limitations

This study will remain at the unclassified level and use open sources to determine the level of threat and protection available to computer networks. This eases handling restrictions while providing an ersatz approximation of a study performed within a civil organization. This is important since a greater share of IO is emerging from the “black” world of secret policy. Therefore, the roles and budget allocation provided for IO are increasingly determined in open source congressional debate. IO consists of a broad range of capabilities including, among others, psychological operations (PSYOP), information security, communications security, physical attack, and electronic warfare.[21] This study narrows its focus to CNA. CNA consists of “operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.”[22] This study will not delve into the issue of IW arms control due to the implausibility of verification. Instead, this study will remain focused on the issue of sovereignty concerning the medium of information. This study assumes that computer forensics will improve to the point where the source of attacks can be verified.

Notes

1. John D. Jones and Marc F. Griesbach, eds., *Just War Theory in the Nuclear Age* (Lanham, Md.: University Press of America, 1985), 3–34; see also A. J. Coates, *The Ethics of War* (Manchester, U.K.: Manchester University Press, 1997), 3.

2. Contemporary books on the subject include Michael Walzer's *Just and Unjust Wars* (1977), Barrie Paskins and Michael Dockrill's *The Ethics of War* (1979), and Michael Howard, George Andreopoulos, and Mark Shulman's *The Laws of War* (1994).

3. Michael Howard, George J. Andreopoulos, and Mark R. Shulman, eds., *The Laws of War: Constraints on Warfare in the Western World* (New Haven, Conn.: Yale University Press, 1994), 2.

4. Nico Schrijver, "The Use of Economic Sanctions by the UN Security Council: An International Law Perspective," in *International Economic Law and Armed Conflict,* ed. Harry H. G. Post (Boston: Martinus Nijhoff Publishers, 1994), 123.

5. Ibid., 127.

6. Ibid.; see also Jonathan Kirshner, *Currency and Coercion: The Political Economy of International Monetary Power* (Princeton, N.J.: Princeton University Press, 1995), 228–35.

7. The United Nations, *UN Charter*, United Nations Conference on International Organization, 26 June 1945, Chap. I, Article 2.

8. *UN Charter*, Chap. VI, Article 33.

9. *UN Charter*, Chap. VII, Articles 39–42.

10. Howard S. Levie, *The Code of International Armed Conflict* (New York: Oceana Publications, 1986), 52.

11. Ibid.

12. David M. Ackerman, "Self-Defense Under Article 51 of the United Nations Charter: The Original Understanding," *CRS Report for Congress* (Washington, D.C.: Congressional Research Service, Library of Congress, 1994), CRS-6.

13. *UN Charter*, Chap. VII, Article 51.

14. Ackerman, CRS-9.

15. David S. Alberts and Daniel S. Papp, eds., *Information Age Anthology*, vol. 1, four parts (Washington, D.C.: National Defense University, 1997), 34.

16. Ibid., 27–75.

17. Ibid., 72.

18. Ibid., 7.

19. Ibid., 8.

20. Ibid., 24.

21. Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, I-10.

22. Ibid., GL-5.

Chapter 2

International Law

At the rate science proceeds, rockets and missiles will one day seem like buffalo—slow, endangered grazers in the black pasture of outer space.

—Bernard Cooper
Gettysburg Review

The features of the media of sea, air, and space combine to describe the information revolution. The sea was the first international medium that could harbor a threat to sovereignty. As an international medium—like the sea before it—the information revolution has greatly improved international communication and enhanced commerce and interdependence. Heavier-than-air flight raised questions of sovereignty to a multidimensional level for the first time. Like Douhet, present-day information devotees claim that information dominance is necessary—and adequate—for victory. Space flight raised the issue of earthly limits on national sovereignty while heralding a realm ostensibly devoted to peaceful uses for the benefit of mankind. Information technology, leveraging space assets and mirroring the space race, is a high-technology field and a source of national pride for those who dominate.

The relationship between a revolution in military affairs (RMA) and national sovereignty is grounded in international law. Changes that threaten national sovereignty precede adaptations of international law. An understanding of the origins of international law and an examination of past revolutions will form the foundation for examining the present RMA.

Roman Law

International law existed as early as the Roman Empire. In addition to conventional treaties with the Jews, Syrians, and Spartans, the Romans recognized a form of unwritten international law. "The Romans knew of a *jus gentium*, a law of nations, which Gaius, in the second century, saw as a law 'common to all men,' a universal law that could be applied by Roman courts to foreigners when the specific law of their own nation was unknown and when Roman law was inapposite."[1] The Roman Empire intended these laws to apply to foreign citizens. Later, in the seventeenth century, Dutch jurist Grotius posited that the law of nations applied to the relationships between states as well. His book, *The Law of War and Peace*, acts as the foundation for the modern discipline of the law of nations. In 1789 English philosopher Jeremy Bentham coined the phrase *international law* to identify the environment Grotius depicted.[2] Unlike municipal law, international law maintains no independent coercive means. However, international law has established a framework that permits the development of sovereign relations not simply based on "might makes right."

The environment that characterizes international law includes conventional law, customary law, and general law. Conventional law is written explicitly—typically in treaty or convention format. It is mutually binding to all states that sign and ratify a pact.[3] As the product of voluntary negotiation and positive action, conventional law is more binding than customary law, which lacks these characteristics. Customary law emerges from state practice where actions "create justifiable expectations of future observance."[4] A third source of international law is the common municipal practice of sovereign states. In cases where there is near universal opinion on a legal issue within the borders of states, "it may be presumed that these rules are so fundamental as to be more or less automatically a part of international law."[5] Within these realms of international law lie two viewpoints as to the necessity of state action (or inaction) to substantiate law.

As politics appears divided between liberals and conservatives, so law is divided between positivists and naturalists. Positivist lawyers generally insist on the positive consent of states to establish understanding. Naturalists argue certain rules "are bound to exist regardless of state consent and that, beyond general principles of law, there are other sorts of nonconsensual rules of international law."[6] In the naturalist exercise of international law, however, it often becomes necessary to examine the contextual elements prevailing at the time of mandate. Negotiating conventional law becomes imperative when differences in cultures or governments tend to distort opinions on customary law. While negotiation adds to the bulk of existing law, it tends to make matters less equivocal.

International legal matters that pose dilemmas have evolved through stages which conclude with written agreements. In these situations international law develops according to a three-stage pattern:

1. Debate forms on a subject with conflicting opinions.
2. Practice of states begin to form customary law (sometimes disputed).
3. States agree to treaty or convention.[7]

Afterwards, if time renders the written law ineffective, a return to step one restarts the process. Sovereignty has been a frequent source of friction between states. In particular, revolutions in methods of transportation have driven examination of prior conventions and, ultimately, the development of new conventional law. The modern examples of maritime, air, and space law provide a solid foundation for examining the present circumstances.

Maritime Law

As the first medium to encounter sovereignty dilemmas not related to territory, maritime law acts as the bedrock for other transportation mediums. Maritime law started developing when the first claims of sovereignty occurred beyond the surf. Primarily for the maintenance of land sovereignty, states attempted to place a buffer zone around their territorial interests. “Such interests included the prevention of poaching on local fishing grounds, prevention of smuggling, control of negligent navigation in coastal waters, and the prevention of other incidents which endangered the inhabitants of the state concerned.”[8] Even after centuries of practice, maritime sovereignty was still a source of dispute in the mid-1940s. Traditionally, states had observed a three-mile limit to their claims of maritime sovereignty, which represented the approximate range of cannon shot when first practiced. Until technology permitted greater exploitation of offshore natural resources, this custom was adequate.

Stage One—Debate

States eventually challenged the customary three-mile limit as they sought to control the natural resources beneath the surface.[9] The United States aggravated maritime peace in 1945 by claiming the natural resources on—and fishing areas above—its continental shelf. This caused reciprocal action by other nations that did not benefit from such an extensive continental shelf. Instead, these states made capricious claims (some exceeding 200 miles) to the extent they were able to exploit.[10] Much of the US position was framed to permit the free economic exploitation of the seabeds, which would reward previous investment by US corporations.

Stage Two—Customary Law

To support US policy, the Navy established an exercise-of-rights program to contest what the United States considered illicit claims.[11] The Navy would intentionally sail ships within claims other states had made, which exceeded the stated US position. A vigorous example of attempting to develop customary law, this program remains an important part of the Navy’s role, highlighted recently by clashes in the Gulf of Sidra to oppose Libyan sovereignty assertions.

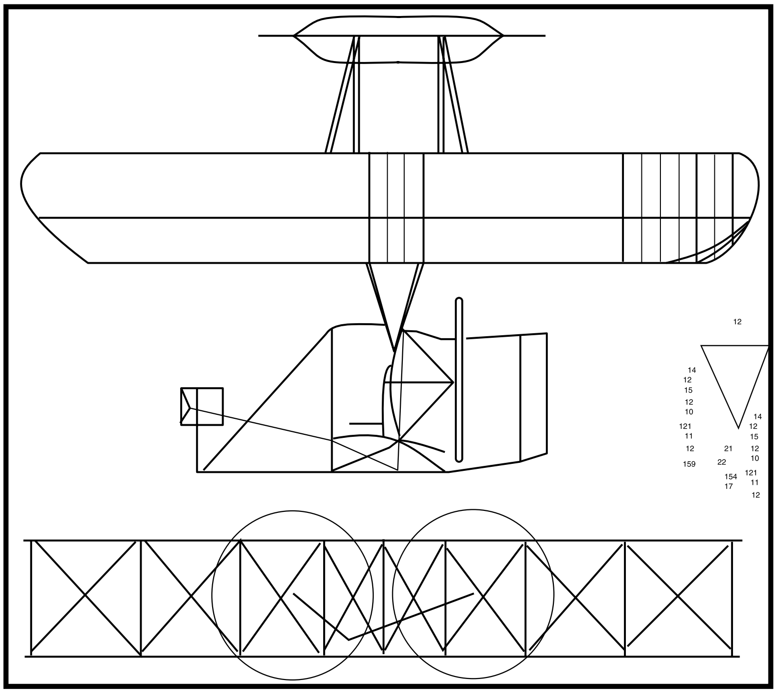
In the meantime, like the land rush days of the US western expansion, states claimed and held what ocean they reasonably could. Other states found it in their interest to recognize only the three-mile limit so that their ships could harvest from the richest fishing areas while ignoring sovereignty claims. Unable to establish zones of fishing conservation, countries clashed over rights to collect fish from the sea and depleted areas once believed everlasting. Oddly, the disputes over customary law caused states to act against their long-term interest. To prevent clashes of military forces and realize the benefits of maritime peace, it became necessary to reach an accord all states could live by.[12]

Stage Three—Conventional Law

The UN International Law Commission started work in 1949 on the UN Convention on the Law of the Sea. The United States agreed with the majority of it but refused to sign it due to the proposed collective administration of seabed natural resources. Other states saw the new "12-mile limit to the territorial sea and the various transit rights guaranteed in the Convention [as] negotiated trade-offs for the Convention's deep seabed mining provisions."[13] Ultimately, the US administration received concessions on seabed mining and approved it in 1998, pending Senate ratification.

Air Law

In contrast to maritime law, conventional law of the air developed more rapidly (perhaps due to fewer natural resource conflicts). Before heavier-than-air flight, maritime analogies were used to describe the air. As far back as 450 B.C., Roman legal opinion stated, "The air should be open to the free use of all, and that it might be used freely as might the flowing water, the sea shores, and the sea."[14] Much later, in 1889, German balloons landing within French territory caused the question of air sovereignty to arise. As relative masters of flight, the French were poised to benefit from a liberal regard for air sovereignty. The French "held that since the air was not susceptible to a regular occupation in its entirety, there could be no ownership of the air."[15] In opposition, the English held that it was not a question of owning the physical air but one of defining the airspace. Controlled flight would provide more incentive for convention (fig. 1).



Source: First Flight Centennial Foundation home page, n.d., n.p.; on-line, Internet, available from http://www.firstflightcentennial.org/foundation.htm.

Figure 1. 1903 Wright Flyer Sketch

The advent of dirigibles and airplanes and their clear military potential led to international custom on air sovereignty. The International Air Navigation Conference, held in Paris in 1910, provided early guidance for state sovereignty in the air. Although nonbinding, it formalized customary law through general agreement that "each state had full sovereignty in the usable space over its national lands and waters, that no general right of international transit existed for aircraft of other states in the absence of international law, and that the only practical legal method of regulating international flight was by agreement which would provide for the grant of privileges of flight through such national airspace."[16] Conduct during World War I solidified the practice of defending sovereign airspace. Nations intercepted and shot down enemy aircraft. Neutral states pursued and forced down belligerent aircraft and interned their crews. "National airspace came to be considered as sacrosanct as sovereignty itself and was no less jealously guarded."[17]

After World War I, conventional law developed to distinguish air sovereignty. The Paris Convention of 1919 recognized exclusive state sovereignty over the airspace above a nation's territory to include the mother country, all colonies, and adjacent territorial waters.[18] The United States chose to reserve its opinion on the issue of air sovereignty, declining to sign the Paris Convention. It seemed that the United States would be in a better position to negotiate later. Indeed, the United States did ratify the Warsaw Convention of 1929 and the Chicago Convention of 1944. These conventions confirmed state air sovereignty and established rules for safety of flight. At the time, although space flight was not yet attainable, debate over space sovereignty developed.

Space Law

The early question of law regarding space dealt with the dividing line between sovereign air and not-so-sovereign outer space. In time, this followed the three-phase model for evolving international law described above. While spacecraft were still mere visions of science fiction writers, early twentieth-century authorities already began to question whether conventions of law in the air would apply in limitless space. Space rhetoric heated up after World War II when the United States and the Soviet Union squared off in a cold war competition for ideological dominance.

Stage One—Debate

Early in the deliberation on space law, the idea of limitless sovereignty projected from terrestrial land boundaries broke down. A satellite "pays little respect to sovereign state boundaries, as its orbit in space remains independent of the earth's rotation and it thereby establishes a new track for each revolution in orbit."[19] Limitless extension of air sovereignty would nearly prohibit the development of satellites. Advocates maintained "an individual earth state would not likely consider an object orbiting about the moon as an encroachment upon its particular territorial sovereignty or national airspace."[20] The idea of sovereignty reaching out to infinity and transferring ownership of extraterrestrial bodies based upon the rotation of the earth was absurd. However, any nation would find overflight of its territory by foreign bombers at 50,000 feet unacceptable. In September 1952 the Third International Astronomical Congress met in Stuttgart, West Germany, and concluded,

> The factors which tend to make the close relationship between the earth and the airspace above it appear to be natural law, do not apply to nonatmospheric outer space, for only the area filled with air stands in such an essential relationship with life on the surface of the earth, that it must be designated as belonging to the earth. Contrariwise, this "special and sovereign correlation" does not exist between outer space and the land and water areas under it. Outer space cannot be considered as an "integral constituent part" of the territory of a state.[21]

The question then became one of dividing lines—where does air end and space start?

The dividing line between air and space was the subject of profound debate. In 1945 Hans Kelsen asserted that for the "efficacy of the national legal order," each state's territorial dimensions should be defined.[22] He proposed using a method that would limit sovereign air boundaries to those within which a state could establish effective control. This method would create a dynamic frontier that would change as technology developed. In 1951 John C. Cooper, former director of the Institute of Air Law at McGill University, tended to agree with "effective control" as a mechanism. He concluded, "the only rational approach was that the limit claimed by the most advanced state should be enjoyed by all states, regardless of their strength."[23] By 1956 he had given up this concept due to the difficulties in application. Instead, he substituted a "trizonal concept" which would "recognize a 'territorial space' upward to the ceiling at which aircraft may be operated; a second zone up to 300 miles called 'contiguous space,' with certain rights for the nations of the world; and a final area above contiguous space called 'free space.'"[24] By 1958 experts recognized the difficulties regarding inspection regimes and orbital transitions between zones, as well as dissension about the intermediate distance between contiguous and free space. Instead, a simpler "bizonal concept" emerged to separate air from space.

Several physical characteristics acted as candidates for the air/space dividing line. The views ranged "from as low as 30 miles to the suggestion that, if the term 'atmosphere' is used, it might extend upward as high as 60,000 miles."[25] More commonly, a proposed 53-mile limit existed as the height where aerodynamic lift is gone but sustained orbit could be maintained. This became known as the "Karman 53-mile line" after the author of the study that proposed it.[26] Ultimately, scholastic deliberation established a baseline for demarcation which practice would have to reinforce.

Stage 2—Customary Law Develops

The 1957 International Geophysical Year (IGY) was an opportunity for the United States and the USSR to cloak their national space efforts with the peaceful development of science. While not tied to internationally sanctioned IGY events, both nations stated their proposed satellite launches would be within the auspices of peaceful scientific research. Officials in President Dwight D. Eisenhower's administration secretly hoped the Soviets would launch first and establish a freedom in space that they could not revoke.[27] The Soviets obliged by launching *Sputnik I* on 4 October 1957. Establishment of customary law required an explicit action, subsequently unopposed. Both nations had proclaimed their intentions to launch earth-orbiting satellites but did not request diplomatic clearances to overfly the sovereign airspace of other states.[28] The fact that no nation protested the satellites would satisfy the naturalists. In this case the silence of other nations was consent. Positivist advocates illustrated how fervently states opposed other acts of airspace violations. "At the same time that satellites are circling the earth in indiscriminate orbits as far as surface territory is concerned, a dozen or more complaints, protests, and international incidents have arisen from claims of violations of national airspace."[29] The presence of objection in one regime (air) and the absence of objection in another (space) established positively that there was a difference. Strangely, in the next 40 years conventional law has not completed the issue by an explicit agreement on an air/space dividing line. Instead, states have seen a more important issue in the *purpose* of man-made space objects.

Stage 3—Conventional Law

In an attempt to maintain the existing balance of power, in the 1960s the United States endorsed a regime that would not permit a destabilizing use of space. With remarkable advances in nuclear weapons mated with missiles, WMD on orbit might be a logical next step. "This system of attack by 'airborne' ICBM poses a much greater threat than that of a free-falling missile initiated from the surface."[30] In an effort to prevent proliferation of this capability, the United States proposed to ban the placement of WMD in orbit and ultimately succeeded with the Outer Space Treaty of 1967.[31] Additionally, the treaty banned the placement of WMD or military installations on any celestial body. It also required states to render all possible assistance to foreign astronauts in distress and provided for inspection of extraterrestrial installations. However, it did not address the issue of conventional weapons in orbit.

Status Quo—Waiting for the Shoe to Drop

As positivists would argue about international law, an act not explicitly banned is permitted. In this sense what is absent from the Outer Space Treaty and other agreements says a great deal. According to a US Army instructional text on space: “International law implicitly permits such traditional military support functions such as surveillance, reconnaissance, navigation, meteorology, and communications [in space]. It permits the deployment of military space stations; the testing and deployment in earth orbit of non-nuclear, non-ABM weapon systems; the use of space for individual and collective self-defense; and any conceivable activity not specifically prohibited or otherwise constrained.”[32]

The weaponization of space is currently a question of policy, not law.[33] Some might argue the pacification of space is implicit in all treaties regarding space, and the lack of weapons in space has created a customary regime that forbids them. However, the absence of any effort to place weapons in space has denied states the opportunity to oppose them.

The Models

International law has codified limits for the sovereign dimensions of land, sea, and air. The unique nature of space leads to issues not seen among terrestrial mediums. Generally, nations cannot object to the military presence of land, sea, or air forces outside their sovereignty. Absent a definitive limit between air and space, conventional law has sought to limit space by purpose or intent. Since space overlays other environments, even those nations unable to launch satellites hold it in high regard. This respect, combined with the deliberate nature of employing in space, permits great detail and care in the evolution of space law. Conventional law awaits customary judgment as to whether outer space is an international free regime, akin to the high seas and international airspace, or one restricted to benevolent use. Like space, information is a pervasive medium. However, rapid development of computer technology and inexpensive operating costs may cause technology to transcend legal precedents.

Notes

[1] Mark W. Janis, *An Introduction to International Law* (Boston: Little, Brown and Co., 1993), 1.

[2] Ibid.

[3] Ibid., 5.

[4] Ibid.

[5] Ibid.

[6] Ibid., 6.

[7] Charles A. Roberts, “Outer Space and National Sovereignty,” *Air University Quarterly Review* XII, no. 1 (Spring 1960): 55–56.

[8] Martin B. Schofield, “Control of Outer Space,” *Air University Quarterly Review* X, no. 1 (Spring 1958): 94.

[9] Ibid.

[10] Ibid., 96.

[11] Janis, 213.

[12] Ibid., 204.

13. Ibid., 213.

14. Schofield, 93.

15. Ibid., 94.

16. Ibid.

17. Roberts, 54.

18. Ibid.

19. Schofield, 97.

20. Ibid.

21. Ibid., 98.

22. Roberts, 56.

23. Ibid.

24. Ibid., 57.

25. Ibid.

26. Ibid.

27. Walter A. McDougall, *The Heavens and the Earth: A Political History of the Space Age* (Baltimore: Johns Hopkins University Press), 186.

28. Schofield, 98.

29. Roberts, 59.

30. Schofield, 100.

31. McDougall, 417–18. The treaty is officially designated as the Treaty on the Principles of the Activity of States in the Exploration and Use of Outer Space Including the Moon and Other Celestial Bodies.

32. *US Army Space Reference Text* (Fort Leavenworth, Kans.: US Army Command and General Staff College, January 1995), 3–9.

33. Bruce M. DeBlois, "Space Sanctuary: A Viable National Strategy," *Airpower Journal* XII, no. 4 (Winter 1998): 41–57.

Chapter 3

Information Reliance

> *Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire, it wafts across the electrified borders.*
>
> —Ronald W. Reagan
> *Guardian*

To alter international law, large constituencies must be convinced that a future with change is better than the status quo. Any additional law or regulation is an agreement to trade freedom of conduct for regulation. The benefits of regulation may include security, predictability (which can lead to efficiency), and impartiality. The costs typically associated with excessive legislation include inefficiency, costs of implementation, and limits on liberty due to boundaries. Before considering a law that governs the use of information, it is imperative to determine the importance of information.

The significance of a national information policy reflects information's importance to society and national defense. American society has markedly increased its reliance on computer technology. The ongoing RMA is the result of technology advances tied to doctrine and organization changes. In response, the *National Security Strategy of the United States (NSS)* and the *National Military Strategy of the United States of America (NMS)* have identified technology reliant infrastructures as being vital to US interests. This chapter examines the importance of both information and infrastructure as their security and efficacy are interdependent.

Information as a Vital US National Interest

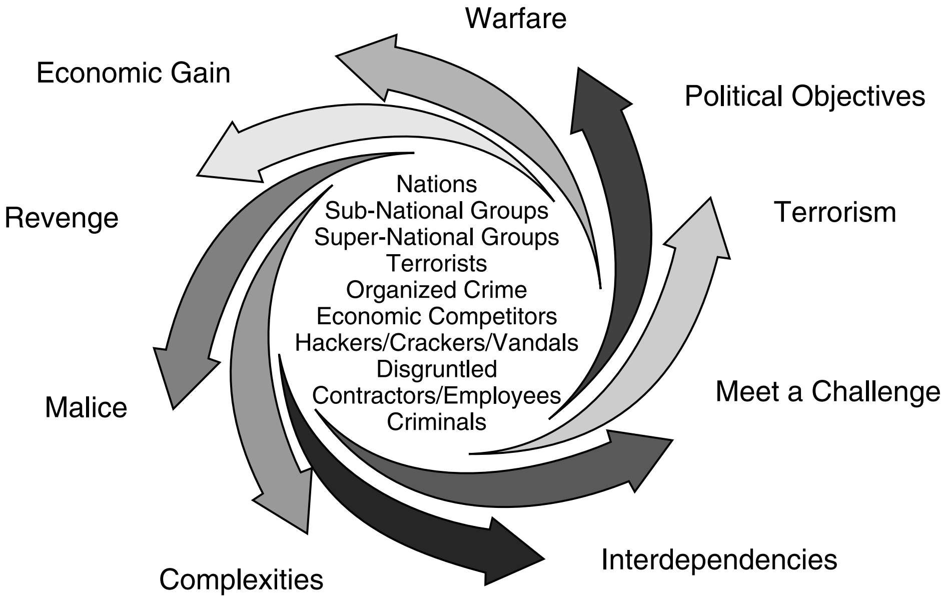
The 1998 *NSS* incorporated changes that elevate the importance of information to US security. In confronting emerging security vulnerabilities, the *NSS* departed from the pattern of posting ordinary changes to a notable update incorporating highlights from the President's Commission on Critical Infrastructure Protection (PCCIP).

Each *NSS* from 1997 and 1998 has themes that act as the foundation for national policy. Specifically, in the preface each delineates three core objectives: to enhance US security, to bolster America's economic prosperity, and to promote democracy abroad.[1] The 1997 *NSS* alludes to national interests throughout the document. However, it does not define national interests nor give explicit examples of them. Instead, the 1997 *NSS* provides six strategic priorities that President William J. Clinton laid out in his 1997 State of the Union Address:

- foster an undivided, democratic, and peaceful Europe;

- forge a strong and stable Asia Pacific community;
- continue America's leadership as the world's most important force for peace;
- create more jobs and opportunities for Americans through a more open and competitive trading system that also benefits others around the world;
- increase cooperation in confronting new security threats that defy borders and unilateral solutions; and
- strengthen the military and diplomatic tools necessary to meet these challenges.[2]

Within the 1997 *NSS*, information is treated as an enabler and not as a national interest in its own right. "The national security posture of the United States is increasingly dependent on our information infrastructures."[3] While the 1997 *NSS* grants that the interdependence within the infrastructure makes it vulnerable, it alludes to concepts and technologies under development for its protection. It further states that the new measures must be fully implemented to ensure future security of "not only our national information infrastructures, but our nation as well."[4] (fig. 2)



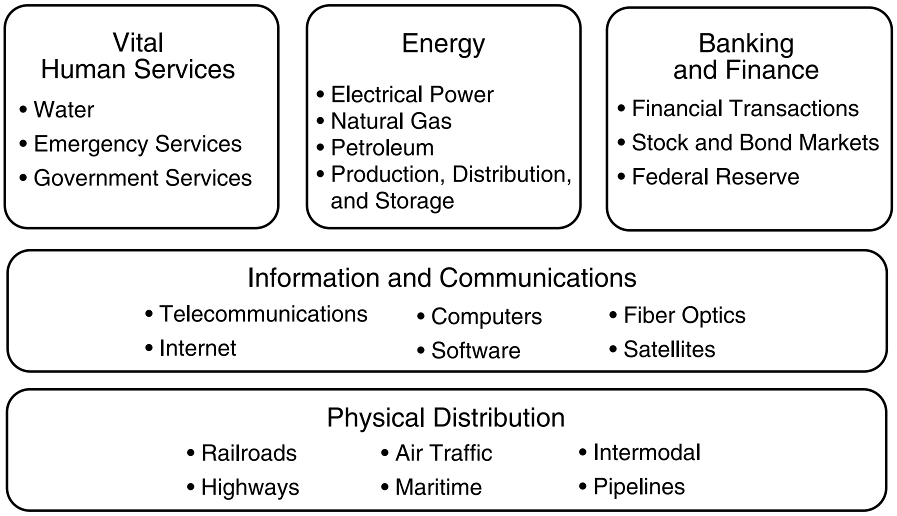
Source: President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures,* October 1997.

Figure 2. Threats, Risks, and Motivations

In contrast the 1998 *NSS* makes the strategic foundation of national infrastructures more explicit. It places critical infrastructures at the forefront of national interests, while explicitly defining what national interests are. In the preface the 1998 *NSS* states, “Protecting our citizens and critical infrastructures at home is an essential element of our strategy.”[5] At first glance it seems to parallel past calls for protecting US citizens within its territory. However, associating citizen protection with infrastructure security is a big step towards justifying a federal responsibility for that security. The 1998 *NSS* adds that “potential adversaries—whether nations, terrorist groups or criminal organizations—will be tempted to disrupt our critical infrastructures, impede government operations, use weapons of mass destruction against civilians, and prey on our citizens overseas.”[6] Equating attacks on critical infrastructures with types of physical aggression seems a drastic change in the policy structure.

In another variance the 1998 *NSS* actually provides the administration’s definition of national interests. It describes three categories of interests, the first of which are vital. Vital interests are “those of broad, overriding importance to the survival, safety and vitality of our nation. Among these are the physical security of our territory and that of our allies, the safety of our citizens, our economic well-being and the protection of our critical infrastructures. We will do what we must to defend these interests, including—when necessary—using our military might unilaterally and decisively.”[7] The *NSS* also identifies the categories of “important national interests” (such as halting the flow of refugees from Haiti and US involvement in the North Atlantic Treaty Organization operations in Bosnia), and “humanitarian or other interests” (responding to natural or man-made disasters, etc.). Conspicuous is the relative importance infrastructure has taken (fig. 3). As a vital interest, it apparently carries greater importance than the Bosnia or Haiti operations and significantly more than a “mere” disaster. Later in the document, under “Emerging Threats at Home,” “Protecting Critical Infrastructures” is second only to “Managing the Consequences of WMD Incidents.”[8] The 1998 *NSS* then translates its vital interest into concrete action.

The new National Infrastructure Protection Center (NIPC) is the designated federal agency in charge of coordinating infrastructure security. The 1998 *NSS* refers to “Presidential Decision Directive 63,” signed in May 1998, which “makes it U.S. policy to take all necessary measures to swiftly eliminate any significant vulnerability to physical or information attacks on our critical infrastructures, especially our information systems.”[9] Consequently, the NIPC will become the focal point for gathering information on threats to the infrastructures.[10] The NIPC will identify and assess threats, provide warnings, and conduct incident response and investigations. However, the NIPC’s lack of international authority will necessitate deterrence of external threats by other means.



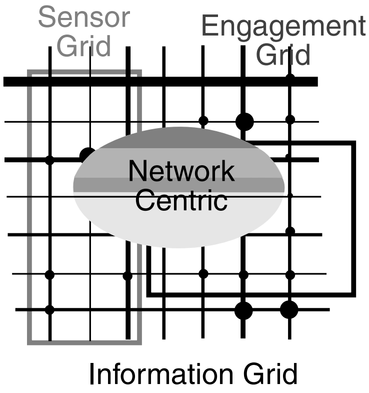
Source: President's Commission on Critical Infrastructure Protection.

Figure 3. Vital Infrastructures

The 1998 *NSS* describes the interdependence and internationalization wrought by the information age. It states, "Globalization is bringing citizens from all continents closer together, allowing them to share ideas, goods and information at the tap of a keyboard."[11] "Protecting our citizens and critical infrastructures at home is an intrinsic and essential element of our security strategy. The dividing line between domestic and foreign policy is increasingly blurred. Globalization enables other states, terrorists, criminals, drug traffickers, and others to challenge the safety of our citizens and the security of our borders in new ways."[12] The declaration of infrastructures as vital is an explicit signal that the United States will protect them.

Information as a Vital Military Interest

The US military exceeds the simple axiomatic urge, typified by Sun Tzu's celebrated quotation, to achieve pervasive understanding.[13] No longer satisfied with scrutinizing the field of combat better than the adversary, the US military relies on superior information technology to convert knowledge into combat effectiveness (fig. 4). In addition to traditional information security, the US military is prepared to conduct offensive IO to degrade an information-dependent enemy's awareness.

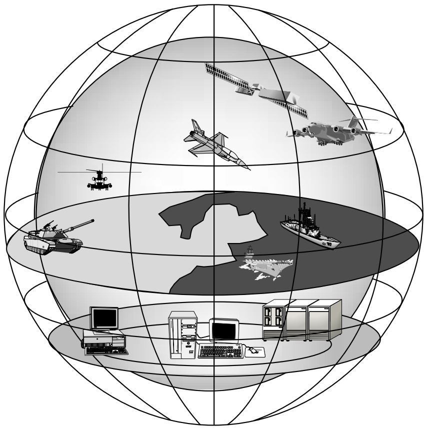


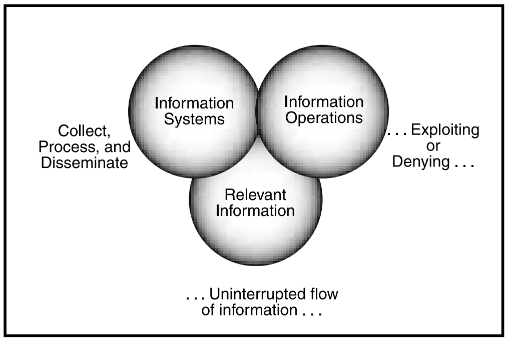
Source: US Atlantic Command.

Figure 4. Military Network

Present Day—National Military Strategy

The 1997 *NMS*, subordinate to the 1997 *NSS*, does not take the leap into information security that appears in the 1998 *NSS*. However, it recognizes the importance of information in securing the objectives of the 1997 *NSS*. It states that the military works "to Shape the international environment and Respond to the full spectrum of crises, while we Prepare Now for an uncertain future."[14] In the shaping of the international environment, information sharing and military-to-military contacts promote trust and confidence; transparency measures in support of arms control reduce tensions and dangers. However, conventional war-fighting capabilities are "the military's most important contribution to the shaping element of the president's strategy" as well as responding to crises.[15] As for the uncertain future, the 1997 *NMS* refers to *Joint Vision (JV) 2010* as the "template for joint operations and warfighting in the future," which "rests on the foundations of information superiority and technological innovation."[16] (figs. 5 and 6)




Information Systems
Information Operations
Relevant Information
Collect, Process, and Disseminate
. . . Exploiting or Denying . . .
. . . Uninterrupted flow of information . . .

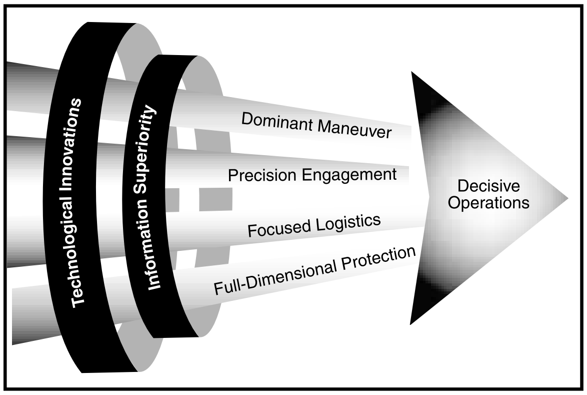
Source: Joint Warfighting Center, *Concept for Future Joint Operations,* 1997.

Figure 5. Global Grid

Figure 6. Components of Information Superiority

The Future—*Joint Vision 2010* and the *Concept for Future Joint Operations*

Information superiority is imperative to joint force success in the future envisioned by the chairman of the Joint Chiefs of Staff (CJCS). *JV 2010* is the CJCS model for future joint war fighting. The *Concept for Future Joint Operations* (*CFJO*) follows with a detailed look at how the services will proceed to meet *JV 2010* operational goals. *JV 2010* defines information superiority as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[17] The success of *JV 2010* relies upon "emerging technologies—particularly information-specific advances" to permit increased effectiveness. The four essential operational concepts of dominant maneuver, precision engagement, full-dimensional protection, and focused logistics will demonstrate this effectiveness (fig. 7). In describing these concepts, the *CFJO* builds heavily upon the assumption of information control.



Information Superiority and Technological Innovation

End States

- Economy of force
- Higher tempo
- Increased stealth, mobility, flexibility
- Ability to integrate all systems—sensors, C^2, weapon platforms, etc.
- Improved C^2 and collaborative planning systems

Source: Joint Warfighting Center, *Concept for Future Joint Operations.*

Figure 7. Decisive Operations

The *CFJO* asserts that the synergy between the four operational concepts, supported by abundant data streams, will permit decisive operations. Separately remarkable, their interdependence requires that each succeed. "The JFC, for example, cannot conduct dominant maneuver, full-dimensional protection, and precision engagement for extended periods without focused logistics. Likewise, focused logistics is not possible in combat operations without the umbrella of full-dimensional protection."[18] Sifting through the hyperbole, however, reveals the specific information requirements are merely traditional intelligence needs regarding friendly, enemy, and terrain conditions. The call for rapid and accurate intelligence to minimize the decision cycle is chronic. Unique, however, is the reliance on information systems to supplant, and perhaps replace, existing forms of human intervention. "Traditional graphic control measures—such as the fire support coordination line and unit boundaries" can be "supplanted by information-based methods," enabling dominant maneuver.[19] Automated targeting and response drives precision engagement. Data-intensive system transparency permits focused logistics to achieve, not just-in-case inventory management, but tailored, just-in-time sustainment. Full dimensional protection requires the ability to "see the battle space, to discriminate friend from foe, to anticipate and rapidly counter enemy actions, and to quickly disseminate threat information to all forces."[20] Full spectrum dominance—having supplanted human beings with data streams—sinks or swims on the reliability of information. To satisfy the balance sheets, a reduction in the size of the US military is supposed to pay for the *JV 2010* transition. Therefore, an inability to secure information dominance could result in a future with a smaller—perhaps less capable—force.

Fragility of Information

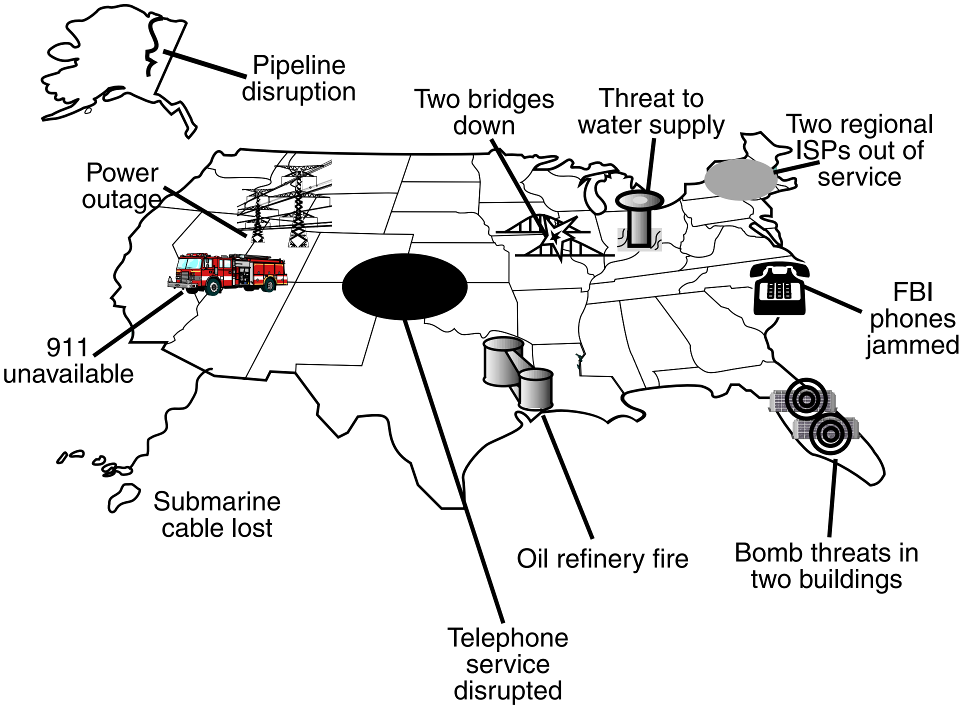
Rhetoric has provided dire visions of computer hackers, viruses, and Y2K. In his best selling novel, *Debt of Honor*, Tom Clancy describes how a rogue element of the Japanese government reduces the electronic transfers of the New York Stock Exchange to worthless garbage, destroying consumer confidence. Actual events have served to heighten fear of exposure. A satellite failure caused half the United States to lose its beeper service and halted companies' ability to process credit card purchases. Hackers replaced contents of Air Force and major media home pages with content ranging from pornography to political statements. The Melissa virus jammed electronic switchboards throughout the country. While fears of a Y2K meltdown are somewhat overwrought, insidious dependency on computer networks has left the United States susceptible to a coordinated information attack.

In its report PCCIP provides what appears to be the blueprint for changes to the 1997 *NSS*. American lives are full of assumptions that things ordinarily work. When an alarm wakes someone up, when a telephone is used, when checks are written and bills paid, the "national infrastructure" acts as the conduit for transactions. The PCCIP determined that there are several infrastructures which "are so vital that their incapacity or destruction would have a debilitating impact on our defense and economic security."[21] These vital infrastructures include transportation, oil and gas production and storage, the water supply, emergency services, government services, banking and finance, electrical power, and telecommunications. Given increased reliance on automation, the report contends that these systems are vulnerable to physical and information attacks and real threats to them from individuals and nonstate actors exist.[22]

A power outage in San Francisco, California, pointed out the fragility of just one piece of the national infrastructure. On 8 December 1998, a mistake by a Pacific Gas and Electric (PG&E) employee caused a cascading array of failures which left the city of San Francisco without primary power for six hours.[23] There were great costs involved in the inadvertent shutdown. Beyond simple quality of life issues, the city's hospitals had to refuse elective surgeries for that day due to a lack of primary power. A woman died after a hit-and-run accident due to inoperative traffic signals. The city of San Francisco lost the interest on "the $30 million to $40 million in property taxes it takes in each day because it was unable to put the money in the bank." San Francisco also paid overdraft bank charges as the result of the absent deposits. That San Francisco maintains less than a day's worth of money in the bank shows how dependent society has become on electronic transactions and gives Y2K zealots a reason to clamor. Trading halted at the Pacific Stock Exchange nearly all day. In the next three days, PG&E responded to 3,000 claim form requests for damages to businesses and individuals.[24] While exposure to litigation drives an awareness of infrastructure protection in the corporate world, the US military remains concerned with national security.

Network Vulnerability

The level of US exposure to a hostile computer attack that would severely degrade the critical infrastructure or military capability is unclear. Military-sponsored think tanks warn that cyberterrorists could "destabilize and eventually destroy targeted states and societies."[25] Cynics view these reports as advertisements for the self-aggrandizing information warfare/computer security industry. Typical citizens, already intimidated by computers and frustrated with "general protection faults," may be inclined to believe that vulnerability is not overblown (fig. 8).



Source: President's Commission on Critical Infrastructure Protection.

Figure 8. Hypothetical Information Attack

The United States Is Vulnerable

Popular information-war scenarios imagine a coordinated attack destabilizing the US infrastructure while other weapons deliver the knockout blow. In an oft-repeated conclusion to a Pentagon report:

> Information warfare specialists at the Pentagon estimate that a properly prepared and well-coordinated attack by fewer than 30 computer virtuosos [sic] strategically located around the world, with a budget of less than $10 million, could bring the United States to its knees.
>
> Such a strategic attack, mounted by a cyberterrorist group . . . would shut down everything from electric power grids to air traffic control centers. A combination of cyberweapons, poison gas, and even nuclear devices could produce a global Waterloo for the United States.[26]

Sen. Fred Thompson (R-Tenn.), a member of the Senate Governmental Affairs Committee, named "China, Russia, Libya, Iran, Iraq, and at least seven other countries" as incorporating IW into their military doctrine.[27] Thompson warned, "we cannot wait for an electronic Pearl Harbor or Oklahoma City to recognize there is a problem."[28] Congressional response to the Y2K bug has heightened awareness of computer dependence. Sen. Robert Bennett (R-Utah) and Sen. Chris Dodd (D-Conn.) issued warnings about "one of the most serious and potentially devastating events this nation has ever encountered."[29] The senators confirmed the possibility of malfunctioning missiles, medical equipment, brownouts, and lost bank records. IW experts are touting Y2K as the first "scheduled cyber-attack," which should be studied to improve response for the next unscheduled one. Multiple hacker success stories, highlighted by celebrated web page alterations, have increased public fear of cyberexposure.[30]

Cyberskepticism

Nonconformist computer experts treat such information-war threat scenarios as "computer-age ghost stories," and note a lack of evidence.[31] In particular they deride the apparent cult status of Alvin Toffler within the national security establishment. Steven Metz of the US Army War College derides the hyperbole of Toffler's book, *War and Anti-War*, as a superficial "MTV clip."[32] George Smith, the editor of *Crypt Newsletter*, an on-line journal dedicated to debunking information age myths, puts it: "One of the strong suits of information warriors appears to be the burying of the enemy with floods of vague military philosophy, impenetrable jargon, cliches, scenarios, and aphorisms gathered from popular books attributed to Alvin Toffler, Tom Clancy, and Sun Tzu."[33] Smith points out erroneous research, performed by presumed experts, which received no subsequent retractions. Federal Bureau of Investigation (FBI) articles have included information originally intended as a joke, such as the rerouting of White House phone calls to the imaginary Marcel Marceau University for Miming, or a nonexistent virus called "Clinton."[34] Other officially propagated hoaxes include warnings to avoid even opening E-mails with certain titles.[35] The reported number of intrusions is multiplied due to assumptions about the poor efficacy of detection. Figures are further inflated by the classification of certain benign system interrogations, or “pings,” as hostile. A lack of Pentagon candor in explaining IW scenarios further aggravates a cynical computer underground.[36] Skeptics point to the lack of significant attacks by an enemy, such as Iraq or Osama Bin Laden, as evidence that the hysteria is excessive.

Information Stress

The increasing use of information and technology in US society has led to a dependence which people are loath to relinquish. Presently, the absence of a significant computer attack may be evidence of superior US defensive IW—not a lack of exposure. Prudence dictates that the US practice safe computing. In time, the evolving realm of customary law will respond to intentional acts of computer hostility. Given the importance of information to the United States, it may be compelling to accelerate the development of international law.

Notes

1. *A National Security Strategy for a New Century* (Washington, D.C.: White House, May 1997), i.

2. Ibid., 2.

3. Ibid., 12.

4. Ibid.

5. *A National Security Strategy for a New Century*, October 1998, iv.

6. Ibid.

7. Ibid., 5.

8. Ibid., 20.

9. Ibid.

10. See figure 3 for a complete list of the President’s Commission on Critical Infrastructure Protection (PCCIP) infrastructure sectors.

11. *A National Security Strategy for a New Century*, October 1998, 1.

12. Ibid., 2.

13. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford: Clarendon Press, 1963), 84. Sun Tzu is an oft-quoted military theorist from ancient China. Among his most attributed quotes is the following, “Therefore I say: Know the enemy and know yourself; in a hundred battles you will never be in peril.”

14. Chairman of the Joint Chiefs of Staff (CJCS), *National Military Strategy: Shape, Respond, Prepare Now—A Military Strategy for a New Era* (Washington, D.C.: Pentagon, 26 November 1997), n.p·; on-line, Internet 20 May 1999, available from http://www.dtic.mil/jcs/nms (hereinafter referred to as 1997 *NMS*).

15. Ibid.

16. 1997 *NMS*; see also CJCS, *Joint Vision 2010* (Washington, D.C.: Pentagon, 1998), Introduction.

17. Commander, Joint Warfighting Center, *Concept for Future Joint Operations* (Fort Monroe, Va.: Joint Warfighting Center, 1997), Foreword.

18. Ibid., 48.

19. Ibid., 50.

20. Ibid., 53.

21. *Critical Foundations: Protecting America's Infrastructures* (Washington, D.C.: PCCIP, October 1997), 3.

22. Ibid., 5.

23. Erin McCormick and Elizabeth Fernandez, "System Failures Widened Blackout," *San Francisco Examiner*, 12 December 1998; on-line, Internet, *The Gate*, available from http://www.sfgate.com, 14 December 1998.

24. Victoria Colliver and Jacob H. Fries, "Losses from PG&E Bungling Adding Up," *San Francisco Examiner*, 10 December 1998, section A1; on-line, Internet, *The Gate*, available from http://www.sfgate.com/cgi-bin/article.cgi?file=/examiner/archive/1998/12/10/NEWS7342.dtl, 28 March 1999.

25. Nancy Weil, "Think Tank Warns of Cyberterrorist Plots," *PC World News*, 16 December 1998, n.p.; on-line, Internet, 28 March 1999, available from http://www.pcworld.com/pcwtoday/article/0,1510,9056,00.htm.

26. Ibid.

27. Gregory Slabodkin, "Senate Kills Info Warfare Funds in DOD Spending Bill," *Government Computer News*, 20 July 1998, n.p.; on-line, Internet, 28 March 1999, available from http://www.gcn.com/gcn/1998/July20/8A.htm.

28. Ibid.

29. Vincent Morris, "Stocking Up for the Y2K Bug Gets Bipartisan Support," *Fox News Online*, 1 March 1999, n.p.; on-line, Internet, 28 March 1999, available from http://www.foxnews.com/scitech/background/y2k/y2k030199.sml.

30. Along with the great coverage of the Melissa virus, there are numerous examples of hacked government web pages. See http://www.onething.com/archive/or http://www.hackernews.com/archive/crackarch.htm for archived examples.

31. "Future Schlock," *Foreign Policy*, no. 113 (Winter 1998–99): 72–87.

32. Ibid.

33. Ibid.

34. George Smith, "An Electronic Pearl Harbor? Not Likely," *Issues in Science and Technology*, Fall 1998, 68–73.

35. The Melissa virus notwithstanding, simply opening an E-mail does not activate a macro virus. For a macro virus to run, one must open the E-mail, then open the attached document, and if standard virus protection is enabled, provide consent for the macro to run.

36. Smith.

Chapter 4

Status Quo—Cyberlitigation

People are getting smarter nowadays; they are letting lawyers, instead of their conscience, be their guide.

—Will Rogers

The development of IW sovereignty has not exactly followed the pattern of other mediums. The United States fostered the nascent computer network grid in relative international isolation. Therefore, the original focus of computer law was domestic, not international. The nature of computer crime allows it to violate multiple jurisdictions instantaneously while the perpetrator may reside overseas. Combined with network anonymity and domestic laws protecting privacy, this makes it extremely difficult to apprehend violators. Since international law lags behind domestic law in this area, this chapter examines the condition of US criminal law.

In dealing with international violations, bilateral agreements have emerged as a precursor to unified international law. Recent scholarship on international law and IW reveals a divided body of opinion. Some insist that current law adequately proscribes international CNA. These people believe that technology and customary law should mature before brokering an international convention. Others assert that current laws, written before the advent of computer networking, are inadequate. A look at the disparate interpretations and the limited body of legal verdicts will shed light on the state of international computer law.

The Cuckoo's Egg

In his book, *The Cuckoo's Egg*: *Tracking a Spy through the Maze of Computer Espionage,* Clifford Stoll describes just how little authorities cared about the occurrence of computer crime in 1987.[1] A "recycled" astronomer at Lawrence Berkeley Laboratory, Stoll's attempt to reconcile a 75-cent shortfall in a $2,387 monthly computer use statement revealed an illegitimate user. Over a nine-month period, Stoll dealt with local and state law enforcement, as well as the FBI, Central Intelligence Agency (CIA), National Security Agency, Air Force Office of Special Investigations, and German authorities in an attempt to track down the operative breaking into his computer system. Each of the agencies at one time or another encouraged Stoll to drop his case in the search for mere change. Not only was the damage apparently minor but none of the agencies could hope to receive credit for "collaring" a computer criminal originating overseas.

Stoll had to justify search warrants for multiple jurisdictions to peel back each computer node by which the hacker had traveled. Ultimately, the user emerged as a group of West German nationals conducting espionage for East Germany. German law did not forbid the types of crimes committed against the US computer systems. The Germans justified their cooperation with the now keenly interested US officials by observing that the hackers had stolen long-distance telephone service. In coordination, a sting operation finally caught the espionage ring.

Increased Awareness

Due to incidents similar to Stoll's, legislation responded to some of the domestic loopholes in computer law; and bilateral agreements emerged to fill some international gaps. Individual criminal activity has received media attention and placed computer crime in the spotlight. Present domestic laws provide the FBI with greater authority in pursuing cybercriminals. In February 1995 the FBI arrested Kevin Mitnick, a phone "phreak" (long-distance service thief) and hacker, long celebrated within the computer underworld.[2] The Department of Justice (DOJ) established the NIPC (described in chapter 3) as part of increased efforts to combat computer crime. International and interagency agreements have improved as well. For example, on 18 March 1998 DOJ announced the following: "The Department of Justice, in conjunction with the FBI, the Air Force Office of Special Investigation, the National Aeronautics and Space Administration and the Naval Criminal Investigative Service, announced today that the Israeli National Police arrested Ehud Tenebaum, an Israeli citizen, for illegally accessing computers belonging to the Israeli and United States governments, as well as hundreds of other commercial and educational systems in the United States and elsewhere."[3] US Attorney General Janet Reno warned that the United States would pursue hackers "around the world and in the depths of cyberspace."[4]

The arrest was downplayed in Israel, where Tenebaum was generally referred to as a childish prankster and admired by Israeli Prime Minister Benjamin Netanyahu as "da-- good . . . very dangerous, too."[5] Tenebaum's lawyers insisted that the Pentagon should be thankful he revealed the flaw in their computer systems before a spy did. Even with new levels of cooperation, the United States had to emphasize the illegal acts he committed against Israeli computer systems. After his arrest Tenebaum became a folk hero, receiving book and movie proposals, television interviews, and a computer endorsement contract.[6] There was conjecture that he would serve his mandatory time in the military working for the Israeli intelligence service. On 9 February 1999, under discreet US pressure, Israel finally indicted him under their domestic law. In the meantime, the United States has little hope for extradition.

Information-war Law: Stage One—Debate

Military attorneys have concluded that existing laws adequately cover IW. In the *Primer on Legal Issues in Information Operations,* the Headquarters US Air Force (USAF) international law division provides,

> The Air Force has adopted the term—"information attack"—to refer to altering information without visibly changing the physical entity within which it resides. Much discussion and debate will be devoted to these subjects in the coming decade or two, but it seems most likely that, in the end, existing legal principles will be successfully extended to these new technologies without the need for much fundamental innovation. However, just as information operations techniques often involve highly complex applications of technology, the legal environment in which they operate often involves similarly complex applications of law. Consequently, informed legal advice at the planning stage of information operations is especially vital. So long as most information operations programs are maintained in special access programs, only attorneys who have been cleared for access to such programs can be involved in providing detailed legal advice.[7]

The primer states that during peacetime, especially within the realm of IO, the definition of a "use of force" becomes complex.[8] It relies on the established precedent of covert action to justify what otherwise would be considered a use of force during peacetime. Within this model the executive branch maintains extraordinary oversight of covert action by the CIA or other agencies. Concerning states' rights to neutrality, the primer allows the importance of delineation between the conditions of peace and war. Ironically, the text then derides the term *act of war* as "a singularly imprecise and unhelpful concept" which is outdated.[9] The primer prefers to focus on the "whole range of less serious breaches of the rights of other nations under international law that still carry significant sanctions for violation."[10] Meanwhile, other opinion attempts to describe the circumstances when *jus ad bellum* or self-defense apply.

Mark R. Jacobson, a doctoral candidate at Ohio State University's Mershon Center, believes the ambiguity in UN charter definitions is tacit approval for open interpretation. "After all, the members of the General Assembly did not consider their list of 'traditional acts constituting aggression,' inclusive of every conceivable form of aggression."[11] In this vein Jacobson believes that "therefore, armed attacks may be those which involve the use of any sort of equipment which enables us to gain a military advantage against our enemy."[12] He concurs with Michael Walzer that a nation has the right to self-defense when a nation perceives the following on the part of an aggressor: "an intent to injure, active preparation making intent a positive danger, and a general situation in which waiting or doing anything *other* than fighting, greatly magnifies the risk."[13] To his credit Jacobson appreciates the classic security dilemma, which provides that enhancing one nation's security is likely to result in another nation's insecurity. In the decision to act within this dilemma, Jacobson asks the aggrieved nation to evaluate the aggressor's "potential for damage, effective range of the enemy weapons and the overall intent of the attack."[14] His confidence in a state's ability to conduct such analysis matches his faith that "the present system of international law will likely prove resilient enough to deal with both new and non-traditional threats."[15]

Lt Col Michael N. Schmitt, deputy chairman of the law department at the US Air Force Academy, adds justification for this assessment. In his essay, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," Schmitt dissects the nuances between IW and traditional kinetic warfare and emerges with a workable international law environment. He concludes that "traditional applications of the use of force prohibition fail to adequately safeguard shared community values threatened by CNA."[16] Arguing for a nontraditional application, Schmitt embraces the flexibility of the UN security regime. He suggests limiting acts in self-defense to de facto armed attacks. His model would increase global stability by limiting the use of CNA.[17]

Regarding the UN charter's stand on the use of force in Article 2(4), Schmitt's framework would proscribe CNA if an attack intends to cause physical damage or human injury or if its effect resembled that of armed force. Schmitt provides room for self-defense under Article 51 for those instances where a computer infraction does not cross the use-of-force threshold but is a precursor to attack. A preemptive act in self-defense is justifiable if it occurs during the last possible window of opportunity and the computer intrusion is an irrevocable step in an imminent and unavoidable attack.[18] He acknowledges that at levels below these thresholds, the Security Council would have to intervene to prevent a breach of the peace. "This may be faint consolation for the State facing a serious computer network attack, but from a world order perspective it represents the optimal alternative."[19] He admits, however, that consensus on a new framework, "let alone its substantive content, is unlikely to gel any time in the near future."[20]

A positivist opinion of existing law finds that ambiguity, heralded by naturalists, is actually a loophole big enough to drive an electronic invasion through. For the purpose of organization, that side of the debate will be represented in the next chapter.

Information-war Law: Stage Two—Customary Law Develops

The body of official and precedent-setting legal decisions on CNA is steadily growing. However, as with the Law of the Sea, different nations are reaching different conclusions. In a significant event heralding the approach of the new millennium, the first (alleged) state versus state information attack recently took place.

The Empire Strikes Back

On 9 September 1998, the Pentagon finally reacted to a CNA with a response in kind; by January 1999 the legal ramifications of that riposte were still unclear.[21] An activist group called the Electronic Disturbance Theater tried to overwhelm the computer network at the Pentagon. Tied to the *Zapatista* rebels in Chiapas, Mexico, the group wanted to respond to what it alleged was US support for the Mexican government. Each time someone logged onto the Electronic Disturbance Theater web page it automatically downloaded a small Java applet to their computers, which initiated repeated access requests to Defense*LINK*. In this fashion the efforts of many combined in a unified attempt to overwhelm the Pentagon server. The Pentagon responded in kind. "Once an attacker was identified, the Pentagon's computers sent a program back to the activist's computer that shut down his or her Web browser, ending the attack."[22] The Pentagon cyberwarriors were not immediately aware of the threshold they had crossed.

Proving that the military needs guidance in IW law, the Pentagon created a legal team to steer "through the often murky waters of information warfare."[23] The team will be part of the Joint Task Force for Computer Network Defense, stood up on 30 December 1998 to maintain constant surveillance of Department of Defense computer systems. Stepping back from previous actions, the task force is to serve purely as a defensive force. The task force is "prohibited from engaging in offensive information warfare operations like the episode of Sept. 9."[24] However, the task force commander, Air Force Maj Gen John H. Campbell, concedes there are a lot of gray areas between offensive and defensive methods. "The gray areas will need to be resolved on a case-by-case basis. There will always be cases where active measures are beneficial."[25] The task force will coordinate responses to CNAs by the various computer emergency response teams.

While the Pentagon seeks ways to passively defend its domain, jurisprudence overseas may be creating a hacker's haven. On 15 December 1998, Norway's Supreme Court ruled that "trying to break into a computer over the Internet is not a crime until the system is actually breached."[26] The Norwegian court stated that those who connect to the Internet are responsible for protecting themselves. The judgment came in response to a case against an Oslo-based computer security firm. The firm, Norman Data Defense Systems, attempted to breach the University of Oslo's computer security as part of a news report for the Norwegian state broadcasting network. The court dismissed a lower court ruling, reasoning that the company had not broken into the network but had just discovered how to do it.

In what may prove to be the first documented case of state-sponsored IW, an Irish Internet provider—hosting East Timor's web domain—is accusing Indonesia of attacking its computer servers.[27] East Timor, occupied by Indonesia since 1975, declared its "virtual independence" in 1998 with the administration of its own top-level domain, ".tp."[28] After the launch of the East Timor domain, the Indonesian embassy relayed its concern to the *Irish Times* about the misuse of computer freedom to campaign against Indonesia. Connect-Ireland, the Irish server that hosted the domain, was the focus of a coordinated attack during late January 1999. The server's project director, Martin Maguire, asserted, "There were 18 simultaneous attacks on our server by robots trying to claw down our defenses."[29] Once in, crackers set up their own domain, "need.tp," with the possible aim of using it for propaganda against East Timor. In spite of uncertainty as to the origin of the attack, Connect-Ireland placed the blame directly on the Indonesian government. Since the attack the UN has brokered a vote for greater autonomy for the territory, which was scheduled in 1999.[30]

Location of Information Warfare on the International Law Continuum

The evolution of IW law is deep into stage one (opinion) and has entered into stage two (custom). Stoll's book still rings true and is a guide for the greater problems faced today. Computer program authors are in a security dilemma. Announce a pressing security need openly, and the customers panic or lose faith. Be discreet, and the system managers ignore it as unimportant.[31] Privacy issues prevent digital identification and pursuit of criminals without a court order from each jurisdiction. In the international realm, each jurisdiction may interpret the issue differently, further complicating the matter. With multiple competing agendas, a workable agreement on a legal interpretation would likely enthuse no one and provoke many. The question remains—Is a future with convention better than the status quo?

Notes

1. Clifford Stoll, *The Cuckoo's Egg*: *Tracking a Spy through the Maze of Computer Espionage* (New York: Doubleday, 1989).

2. Tsutomu Shimomura, *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw—By the Man Who Did It* (New York: Hyperion, 1996), 232–44.

3. Department of Justice, "Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers," *DOJ Press Releases*, 18 March 1998, n.p.; on-line, Internet, 28 March 1999, available from http://www.usdoj.gov/opa/pr/1998/March/125.htm.html.

4. Tania Hershman, "Cracker Indicted: Surprise!" *Wired News*, 10 February 1999, n.p.; on-line, Internet, 28 March 1999, available from http://www.wired.com/news/topstories/0,1287,17850,00.html.

5. Brian McWilliams, "Pentagon Hacker Arrested in Israel," *PC World.Com*, 19 March 1998, n.p.; on-line, Internet, 28 March 1999, available from http://www.pcworld.com/news/daily/data/0398/980319173734.html.

6. "Analyzer Takes Notoriety to the Bank," *Wired News*, 7 April 1998, n.p.; on-line, Internet, 28 March 1999, available from http://www.wired.com/news/technology/0,1282,11534,00.html.

7. Headquarters United States Air Force, Judge Advocate General, International Law Division (Headquarters USAF/JAI), "A Primer on Legal Issues in Information Operations," instructional document (Washington, D.C.: Headquarters USAF/JAI, 1998), 14.

8. Ibid., 16.

9. Ibid., 17.

10. Ibid.

11. Mark R. Jacobson, "War in the Information Age: International Law, Self-Defense, and the Problem of 'Non-Armed' Attacks," *Journal of Strategic Studies* 21, no. 3 (September 1998): 1–23.

12. Ibid., 12.

13. Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 2d ed. (New York: Basic Books, 1992), 81.

14. Jacobson, 22.

15. Ibid.

16. Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," draft prepared for *Columbia Journal of Transnational Law*, 1998.

17. Ibid., cover.

18. Ibid.

19. Ibid., 36.

20. Ibid., 35.

21. Brian Friel, "DoD Launches Internet Counterattack," *GovExec*, 18 September 1998, n.p.; on-line, Internet, 28 March 1999, available from http://www.govexec.com/dailyfed/0998/091898b1.htm; and George I. Seffers, "Legalities Cloud Pentagon's Cyber Defense," *Defense News*, 15 January 1999, n.p.; on-line, Internet, 28 March 1999, available from http://ebwest.dtic.mil/Jan1999/s19990120cyber.htm.

22. Friel.

23. Seffers.

24. Ibid.

25. Ibid.

26. Doug Mellgren, "Norway Court Backs Internet Hackers," *InfoWar*, 15 January 1999, n.p.; on-line, Internet, 28 March 1999, available from http://www.infowar.com/hacker/99/hack_011599d_j.html.

27. Niall McKay, "Indonesia, Ireland in Info War?" *Wired News*, 27 January 1999, n.p.; on-line, Internet, 28 March 1999, available from http://www.wired.com/news/news/politics/story/17562.html; and MSNBC, "Virtual Country 'Nuked' in Cyberwar," 28 January 1999, n.p.; on-line, Internet, 28 March 1999, available from http://www.msnbc.com/news/236038.asp.

28. Brenda Frink, compiler, *Internet Complete* (San Francisco: Sybex Inc., 1998), 15. "Domain names are typically two- or three-character designations of the type of institution or organizations that own the domain." "Countries outside the U.S. use a two-letter country code as their domain name."

29. MSNBC.

30. "U.N. Wants Australian Help in East Timor Vote," *CNN Interactive*, 14 March 1999, n.p.; on-line, Internet, 28 March 1999, available from http://cnn.com/WORLD/asiapcf/9903/14/australia.etimor.01/index.html3.

31. Stoll, 284.

Chapter 5

The International Regime for Information Security Model

To debate the appeal of international convention on CNA, it is necessary to develop a model for one. Since a legal model represents a work in progress, its limits will differ from a final solution. In space law the merits of delineating sovereignty were largely the same for each of the proposed limits, differing only by degree. Similarly, the advantages and disadvantages of an IW model relative to the status quo should remain the same, only changing by degree. Just as early space law debate established a need for air sovereignty limits, an examination of the proposed information regime will determine if convention is desirable.

The International Regime for Information Security (IRIS) model mirrors the sanctuary of a weapons-free outer space without limiting weapons proliferation. Space is a capital-intensive medium, prone to long development, where operations are difficult to conceal. Information weapons get cheaper by the day and can be concealed in the mind of one person, such as Mitnick. Within the IRIS model, the proliferation of information weapons is not proscribed, it is assumed. However, the model prohibits the use of CNA in peacetime. In many instances the model simply codifies what appears to be universally accepted customary law. A few definitions are in order before describing the model.

Computer network attack. From Joint Publication (JP) 3-13, *Joint Doctrine for Information Operations*. Consists of "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[1]

Host consent. Physical human response in a manner of acknowledgment (such as a keystroke or mouse click).

Modification. Any software, firmware, or hardware change performed on a computer system.

Passive modification. The placement of programs onto another computer without host consent. Typical uses of passive modification include Java applets, cookies, and data collection packets. There are many advantages to passive modification which include the storage of form data to save time on subsequent site "visits," or of individual preferences to personalize a subsequent browsing occurrence such as "My CNN."

Unrelated data. Information within a computer system that is irrelevant to another program's effectiveness. For example, a Java applet designed to teach a math lesson does not need to know how many Microsoft Word documents are on the host computer. To the Java applet, the number of Word documents is *unrelated data*.

Blocking software. Software, normally part of the network program, which limits passive modification. Scalable to levels of security, blocking software restricts the types of passive modification permitted on a system. For example—the Netscape and Microsoft browsers can limit acceptance of cookies or Java applets independently to “always accept,” “prompt to accept,” or “always reject.”

The following fundamental guidelines would exist under a peacetime IRIS regime.

1. Boundary—A nation’s sovereignty consists of all information networks within or owned by a state—that is telephone circuits, satellites, communication nodes, computer systems, etc.
2. Freedom of information transfer—With the exception of benign data compression or decompression, no one may modify information in transit or by inaction allow information in transit to become modified.
3. Tampering—No nation may covertly modify any part of an information system external to its boundary.
4. Passive modification blocking—Passive modification is permitted only to systems that have the capability to block it and have elected not to.
5. Prohibited modifications—The following are explicitly prohibited.

   a. Any modification that masks, changes, or allows to be changed, the performance of a system’s blocking software.
   b. Any modification that changes, or allows to be changed, unrelated data without host consent.
   c. Any modification that results in the retrieval of unrelated data to external systems without host consent.

6. Extradition—Nations agree to prosecute individuals or groups that violate this model from within the nation’s boundary or to deliver the transgressors to the aggrieved nation.
7. Aggression—State-sponsored violations of this agreement may be considered an act of aggression under the provisions of the UN charter.
8. Armed force—State-sponsored execution of computer network attack may be considered the use of armed force under the provisions of the UN charter.

Advantages

There are two fundamental advantages associated with the implementation of an IRIS model:

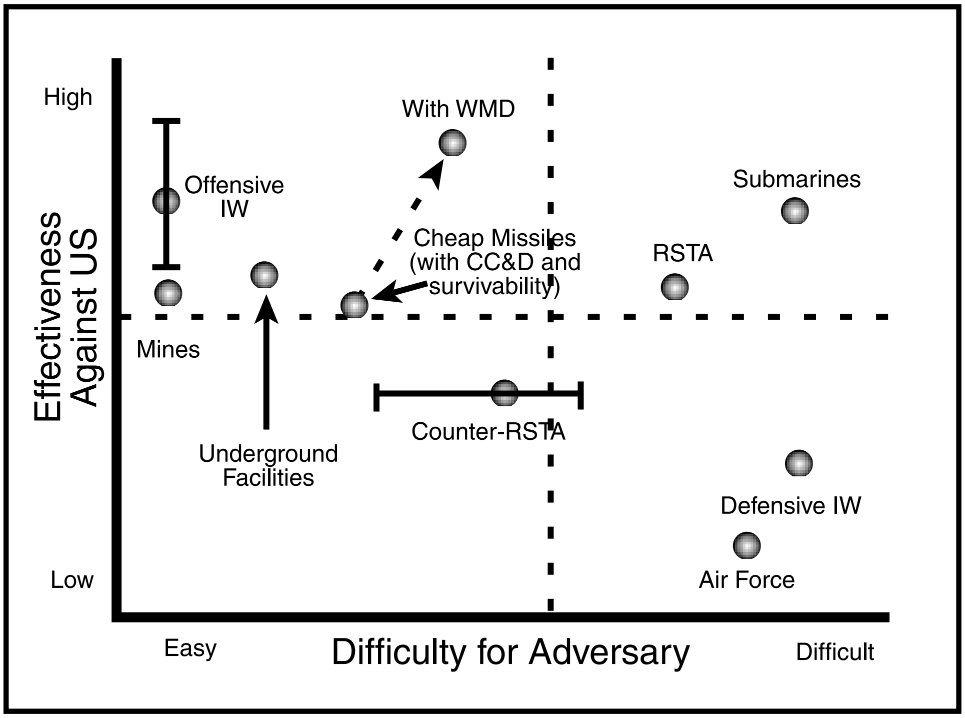
- Increased security in the peacetime information network.
- A change in focus for nascent information warriors.

The main assumption is that adherence to the regime will be universal. The advantages discussed below are examined from a US perspective; however, many of them would directly benefit all nations.

A Protection Regime

Elimination of CNA, as an ideal, would protect vital US information infrastructures. Although the United States would lose the opportunity to take advantage of present legal ambiguity, the regime would benefit the United States overall because it is the nation most dependent on information systems.

> Information age weapons are equalizers. They help small nations against large nations and favor the weak over the strong. Examples include Stinger missiles used by the Mujahedin against the Russians and computer viruses designed to invade individual weapon systems or an entire defense computer network.[2] See figure 9.



Legend:
CC&D—camouflage, concealment, and deception
IW—information warfare
RSTA—reconnaissance, surveillance, and target acquisition
WMD—weapons of mass destruction

Source: Joint Warfighting Center, *Concept for Future Joint Operations.*

Figure 9. Asymmetric Leverage

> The real problem lies in the fact that today's breakthrough technologies in electronics, computer systems, software, and telecommunications come from the commercial marketplace and are available to anyone in the world. Furthermore, foes may use these technologies to their advantage without even resorting to military applications.[3]

In major conflicts the United States has a reputation of waiting to receive the first blow to demonstrate its reluctance to go to war. Due to US reliance on information systems, as illustrated in chapter 3, an information Pearl Harbor could have far greater consequences than did the Japanese attack in 1941.

Crisis Stability

Increasing the reaction time available when conflicts arise will bolster crisis stability. The United States, as the lone world superpower, has much to gain from the maintenance of the status quo. Current IW plans are classified; however, prevalent information war theory anticipates the precursory placement of "time bomb" attack algorithms within an enemy's network. Commercial programs, E-mails, web pages, et cetera, may contain embedded viruses. In renowned nuclear submarine strategy, the ship's captain maintains the launch codes and criteria. If an enemy destroys the national command authority, the submarine can autonomously launch a retaliatory blow. This enhances crisis stability since a knockout first strike is unlikely. Similarly, viruses can be fused to discharge on a certain date, when triggered by a signal, under a certain set of host circumstances, or—if not periodically amended—by a remote "command center." However, the virus's existence within another state's boundary could be as destabilizing as a Trident submarine in the Black Sea. Benign just-in-case viruses, under the wrong circumstances, might become inflammatory reasons for an adversary's preemptive information attack or conventional mobilization. The problem is similar to continental Europe in 1914, as explained by Thomas C. Schelling in *Arms and Influence*. "The steps by which a country got ready for war were the same as the steps by which it would launch war, and that is the way they looked to an enemy. No one can quite say just when the war started. There was a great starting of engines, a clutching and gearing and releasing of brakes and gathering momentum until the machines were on collision course. There was no 'final' decision; every decision was partly forced by prior events and decisions. The range of choice narrowed until the alternatives were gone."[4]

Embedded computer viruses poised to attack the very systems designed for retaliation place a state in a use it or lose it predicament. As with nuclear theory, this creates crisis instability. Furthermore, it is implausible to borrow from nuclear stability theory the creation of explicitly countervalue information weapons since the technology to aim at civilians is that required to aim at forces. In an IRIS regime, the clear communication of rules banning preemptive placement lessens the risks of brinkmanship.

Cultural Agreement While the Iron Is Hot

International settlement of IW issues will ease anxiety about divergent interpretations. US legal experts have great ideas about the applicability of existing law. Unfortunately, it may not be in another nation's best interest to adopt the same conclusion. As transpired with interpretations in maritime law, disputes over virtual sovereignty may lead to squabbles, conflicts, and reprisals. The Norwegian decision allowing break-in attempts short of trespass is a prime example.

> Arne Laukholm, director of Information Technology for the University of Oslo, said the ruling opens the way for systematic and malicious attacks on computers. He said protecting computers hooked up to the global network against such hacking is difficult and expensive.
>
> Dave Farber, a computer expert at the University of Pennsylvania, called it "a bad precedent" that could allow hackers to operate legally in Norway, even if their actions violated other nations' laws.[5]

As with the Law of the Sea, the IRIS regime bridges cultural divides by emphasizing the rewards all will reap in a stabilized system. Meanwhile, the United States can trade its present leverage for future harmony.

US preeminence in IO will tend to wane as time passes. Now, while the iron is hot, is the time to strike an agreement. Samuel P. Huntington, in "The Clash of Civilizations," sees the non-Western world closing the gap in economic and military strength. "Hence the West will increasingly have to accommodate these non-Western modern civilizations whose power approaches that of the West but whose values and interests differ significantly from those in the West."[6] Acting now will capitalize on the West's current edge in political throw-weight as the future "will increasingly be de-Westernized and become a game in which non-Western civilizations are actors and not simply objects."[7]

Interdependence

An IRIS regime will enhance interdependence by reinforcing the global information infrastructure (GII). By decreasing the threat of using information systems, the comfort level with conducting electronic data interchange will increase. Consequently, more states will reach the information age sooner. Increased confidence in the GII will hasten the cycle of economic progress and provide the inherent stability of global prosperity. Taking a passage from the State Department's fact sheet on the Law of the Sea and morphing it into an IRIS essay provides an illustration (changes in italics). See figure 10.

Source: Commission on Global Governance home page, n.d., n.p.; on-line, Internet, available at http://www/ cgg.ch.

Figure 10. Interdependence

> The United States has important and diverse interests in the *realm of information*. As the world's preeminent *telecommunications consumer,* the United States has a national security interest in the ability to freely *transmit data* as essential preconditions for projecting military power. The end of the Cold War has, if anything, highlighted this need. Ensuring the free flow of commercial *information* is likewise a

> basic concern for the United States as a major trading power, whose economic growth and employment is inextricably linked with a robust and growing export sector. By far, the bulk of international trade *relies upon secure data interchange.*
>
> At the same time, the United States, with one of the *largest communication infrastructures* of any nation in the world, has basic resource and environmental interests in *computer security. Online and offline systems* generate vital economic activities—*the internet, academic research,* ports and transportation *automation* and, increasingly, recreation and *gaming.* The *development of knowledge industries* offers the potential for economically and strategically important *data* resources. The health and well-being of *networked* populations—the majority of Americans *use the internet*—are intimately linked to the quality of the *information* environment.
>
> Pursuit of these objectives, however, requires careful and often difficult balancing of interests. As a *cybernetic* nation, for example, we naturally tend to seek maximum control over the *data external to our domain.* Equally, as a major *information* power, we often view such efforts on the part of others as unwarranted limitations on legitimate rights of *transmission.*[8]

Clearly, the advantages of ratifying the Law of the Sea readily transfer to a Law of Information. Some states, taking a strictly realistic view, may see their relative loss instead of their net gain. This is a selfish, outdated view that values rank over abundance. "Unlike the Cold War era, political and economic interdependency in the information age requires cooperation and the open exchange of knowledge."[9]

Simplified Rules of Engagement

Information operations rules of engagement (ROE) would benefit from the clarity provided by convention. Colonel Schmitt's paper does a brilliant job presenting his analysis of how to construe the application of existing law to IW. A codified international agreement based on his framework would be a reasonable solution and rein in uncertainty. However, the fact that it takes more than 50 pages (14,500+ words) for an attorney to explain to other attorneys one possible way to interpret existing law demonstrates how dubious it must seem to commanders not trained in law. Even if it were elementary, wishing other nations would interpret law the same way would not make it so. Schmitt himself characterizes the chances of near-term international agreement on IO law as unlikely.[10]

Through no fault of their own, the Schmitt article and the Air Force's *A Primer on Legal Issues in Information Operations* both must hedge against the absolute applicability of their solutions. An examination of the instances of qualifying words (see table 1) within the main bodies of the two documents sheds light on a reason for pause. For comparison this audit uses four recent *Stanford Technology Law Journal* articles not related to IW. Granted, hypothetical environments make certainty difficult. However, rates of 14.8 and 23.5 percent seem to reflect an underlying ambiguity in international law. Consequently, time spent reaching agreement at "ground speed zero" will pay off when a commander must make a rapid decision to engage. Delineation of where IO crosses the boundary from espionage into aggression or use of armed force will simplify ROE and reduce the time necessary to complete the planning process.

Table 1
Qualifying Word Use

	Schmitt Paper	AF Primer	This Thesis	Stanford Journal
arguably	3	1	0	2
fairly	1	1	0	4
generally	6	6	3	11
likely	18	3	9	12
maybe	13	19	13	19
might	19	10	14	26
most	22	14	12	50
probably	5	7	0	2
Total	87	61	51	126
Sentences	588	260	824	1,139
% qualified	14.8%	23.5%	6.0	11.1%

Intellectual and Fiscal Balance

Openly accepting an IRIS regime will partially disarm IW zealots in their misguided attempts to recreate Douhet’s vision through “command of the infrastructure.” Douhet’s vision of strategic bombardment exaggerated the capability of airpower and led to derision from nonbelievers. IW, with its attendant hyperbole about the electron being the ultimate precision-guided weapon, may suffer the same fate. If present US capabilities were anywhere near their advance billing, a US information war would have convinced Saddam Hussein to abdicate and erased all the secret “how-to” nuclear development documents from North Korean computers.

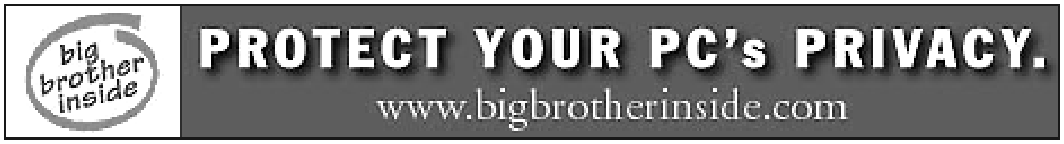
Intellectual balance will also contribute to fiscal balance. While the actual figures are classified, money no longer spent on developing a peacetime CNA can be spent on defensive IO. As with the space race, an IRIS regime would focus the information age competition in the civil, rather than the military, sector.

Disadvantages

Opponents of an IRIS regime focus on what the United States or individuals would lose, rather than gain. Proving that adversity makes strange bedfellows, the IRIS regime would be opposed by civil libertarians, the intelligence community, and the military.

Privacy

Civil liberties groups, such as the Center for Democracy and Technology (see fig. 11), oppose an IRIS regime as an invasion of privacy. For the IRIS regime to be credible, digital identification of communication sources is necessary to prevent anonymous attacks. Privacy advocates reject digital identification as facilitating an Orwellian effort to track the lives of private citizens. Automated data collection is critical to taking advantage of the information revolution, but it can be used for beneficial or harmful purposes. The study of information to examine network performance, improve service, or otherwise assist the consumer is a tremendous benefit of automated retrieval. Conversely, it can be used for "data mining" to target unsolicited advertising or for intelligence gathering to determine system vulnerabilities. Owing to the duality of information, it is not feasible to delineate a universal boundary between good data retrieval and bad. The remaining alternative is to arrange for the selective blocking of data, which the IRIS regime does. Someone not satisfied with that level of protection can also install commercially developed "cyberguard dogs" to sniff out those processes it deems hostile.



Source: Center for Democracy and Technology home page, n.d., n.p.; on-line, Internet, available at http://www.cdt.org.

Figure 11. Digital Identification Backlash

Loss of Sovereignty/Flexibility

Any convention which restricts the use of a type of warfare subordinates national preference to international law and reduces a commander's options. Under an IRIS regime, a commander will have restricted IW options in a low intensity conflict or other circumstances short of war. However, once the threshold of armed force or aggression is crossed, the full range of IW capabilities returns. While this may appear overly stringent, it substantially reflects the current US policy on the use of IW. During the Air Force Doctrine Symposium at Maxwell Air Force Base, Alabama, on 1 March 1999, Brig Gen John R. Baker, Air Force Air Intelligence Agency commander, stated that the US threshold for the use of IW is no less than for traditional kinetic weapons.[11] He stated that IW is treated cautiously in light of WMD analogies, which doubt the ability to limit the effects of an information attack. As a policy decision, current ROE reflect the ambiguous nature of IW. Under an IRIS regime, US policy would be limited by treaty instead of apprehension.

The IRIS regime would be verifiable, enabled by digital identification. Strong encryption would assure the privacy of civil libertarians. The ability to verify the source of attacks through computer forensics aided by digital identification would decrease intelligence needs, balancing the loss of decryption capability. Most importantly, the IRIS model results in the strengthening of US information security and a decreased risk of general conflict due to global prosperity.

Notes

[1] Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October 1988, GL-5.

[2] Lt Col William R. Fast, USA, "Knowledge Strategies: Balancing Ends, Ways, and Means in the Information Age," Institute for National Strategic Studies, n.p.; on-line, Internet, 28 March 1999, available from http://www.ndu.edu/inss/siws/ch1.html.

[3] Ibid.

[4] Thomas C. Schelling, *Arms and Influence* (New Haven, Conn.: Yale University Press, 1966), 221.

[5] Doug Mellgren, "Norway Court Backs Internet Hackers," *PC World Online*, 19 March 1998, n.p.; on-line, Internet, 28 March 1999, available from http://www.infowar.com/hacker/99/hack_011599d_j.shtml.

[6] Samuel P. Huntington, "Clash of Civilizations," *Foreign Affairs*, Summer 1993, 49.

[7] Ibid., 48.

[8] US State Department, "Fact Sheet: U.S. Oceans Policy and the Law of the Sea Convention," Bureau of Oceans and International Environmental and Scientific Affairs, 28 May 1998, n.p.; on-line, Internet, 28 March 1999, available from http://www.state.gov/www/global/oes/oceans/980610_los.html.

[9] Fast.

[10] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," draft prepared for *Columbia Journal of Transnational Law*, 55.

[11] John R. Baker, "Information Operations: Implementing the Doctrine," lecture, Air Command and Staff College, Maxwell Air Force Base, Ala., 1 March 1999.

Chapter 6

The Future

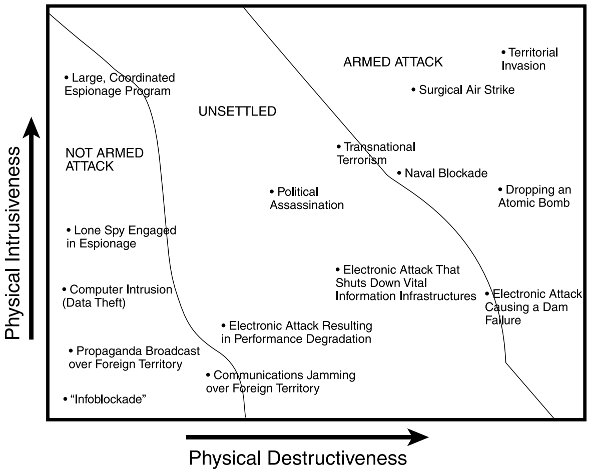
Since wars begin in the minds of men, it is in the minds of men that the defenses of peace must be constructed.

—United Nations Educational, Scientific,
and Cultural Organization, Constitution, 1945

The perception of information as a medium separated from land, sea, and air renders it a disservice. Conversely, simply treating it as an electronic form of communication is naive. Relative information power is not measured in physical terms such as numbers of tanks, ships, or jets. Information is *different*. It has characteristics of land (domain), sea (commerce), air (precision attack), and space (persistence) power. Historical precedents dealing with these realms contain much evidence in attempting to discover a credible international accord.

How We Arrived Here

To narrow the focus, the nature of peaceful relations between states is the focus of this study. Within this a UN convention on international law regarding IO is a logical necessary first step. Saint Thomas Aquinas's examination of *jus ad bellum*, the right to go to war, provides historical depth.[1] As a formal descendent of his work, the Charter of the UN establishes guidelines for the legitimate use of armed force and the peaceful resolution of disputes. The advent of IO, however, blurs the line between peaceful acts and hostile acts.


ARMED ATTACK
• Territorial Invasion
• Large, Coordinated Espionage Program
• Surgical Air Strike
UNSETTLED
NOT ARMED ATTACK
• Transnational Terrorism
• Naval Blockade
• Political Assassination
• Dropping an Atomic Bomb
• Lone Spy Engaged in Espionage
• Electronic Attack That Shuts Down Vital Information Infrastructures
• Computer Intrusion (Data Theft)
• Electronic Attack Causing a Dam Failure
• Electronic Attack Resulting in Performance Degradation
• Propaganda Broadcast over Foreign Territory
• Communications Jamming over Foreign Territory
• "Infoblockade"
Physical Intrusiveness
Physical Destructiveness

Source: Institute for National Strategic Studies.

Figure 12. Classification of Attacks

That information commerce profits from peaceful agreement corresponds to a maritime setting. Meanwhile, information's indistinct boundaries parallel the early days of air and space. The analogies between sea, air, and space provide insight into potential international convention. See figure 12.

Maritime Law

As the first medium to encounter sovereignty dilemmas not related to territory, maritime law acts as the basis for other mediums. To support the maintenance of land sovereignty, states attempted to place a buffer zone around their territorial interests. Maritime law established a three-stage model for international sovereignty:

1. Debate forms on a subject with conflicting opinions.
2. Practice of states begin to form customary law (sometimes disputed).
3. States agree to treaty or convention.[2]

While maritime law was older, it did not firm up until recently with the ratification of the Law of the Sea. It lingered on, at first, due to a lack of interest. As long as a customary three-mile limit applied, nations were happy. Once the resources of the sea became an issue—with fishing and seabed mining rights at stake—nations clamored to grab as large a share of the sea as possible. Recognizing that the benefits of cooperation outweighed the costs of agreement, the United States signed the Law of the Sea in 1998.

Law of the Air

Before heavier-than-air flight, maritime analogies were used to describe the air. Early Roman law opinion included, "The air should be open to the free use of all, and that it might be used freely as might the flowing water, the sea shores, and the sea."[3] Customary law emerged with controlled flight and the conflict of World War I. Nations intercepted and shot down enemy aircraft. Neutral states pursued and forced down belligerent aircraft and interned their crews. "National airspace came to be considered as sacrosanct as sovereignty itself and was no less jealously guarded."[4] The Warsaw Convention of 1929 and the Chicago Convention of 1944 endorsed state air sovereignty and established rules for safety of flight.

Law of Space

When space flight became possible, some commentators proposed to extend state air boundaries to infinity. Oddly, no conventional law since has defined an explicit boundary. Absent a definitive limit between air and space, conventional law has sought to limit space by purpose or intent. In the 1950s the United States endorsed a regime that would not permit a destabilizing use of space. The Outer Space Treaty of 1967 banned the orbiting of WMD, as well as the placement of WMD or military fortifications on any celestial body.[5] As to ordinary weapons, conventional law has not weighed in.[6] Some might argue the pacification of space is implicit in all treaties regarding space, and the lack of weapons in space has created a customary regime that forbids them. However, the absence of any effort to place weapons in space has denied states the opportunity to oppose them.

Conventional law still awaits customary judgment as to whether outer space is an international free regime, akin to the high seas and international airspace, or one restricted to benevolent use.

Information as a Medium

American society has increased its reliance on information technology. Consequently, the US national security strategy and national military strategy have embraced technology-reliant infrastructures as vital to US interests. Differences between recent national security strategies illustrate an emerging dependence. Each national security strategy delineates three core objectives, which are to enhance US security, to bolster America's economic prosperity, and to promote democracy abroad.[7] However, the 1998 *NSS* illustrates the emerging importance of information. In describing national interests, it equates citizens with the critical infrastructures and infrastructure disruption with WMD. The 1998 *NSS* provides validation that information and its relative importance have come of age.

Not surprisingly, the United States relies on superior information technology to convert information into combat effectiveness. *JV 2010,* the CJCS vision, plans to leverage information systems to supplant and, in some instances, replace present forms of human interaction. This greatly speeds up the decision cycle but leaves the US military with a dubious foundation of information superiority. Lacking information dominance, the anticipated smaller, more lethal force may end up being just smaller.

Information Vulnerability

The PCCIP determined that there are several infrastructures that are critical. Due to reliance on information systems, the report contends that vulnerabilities exist to information attacks and that the threat is real.[8] The power outage in San Francisco, California, and the Melissa virus demonstrate the potential fragility of the national infrastructure. However, the true vulnerability of computers is not so clear.

Military-sponsored think tanks warn of apocalyptic events. Sen. Fred Thompson (R-Tenn.), a member of the Senate Governmental Affairs Committee, named several historically adversarial nations as incorporating IW into their military doctrine. He warned, "we cannot wait for an electronic Pearl Harbor or Oklahoma City to recognize there is a problem."[9] However, skeptics view the hype as advertisements for a self-aggrandizing IW/computer security industry. George Smith, the editor of *Crypt Newsletter,* cites FBI articles which included information originally intended as a joke, such as the rerouting of White House phone calls to the Marcel Marceau University for miming, or a nonexistent virus called "Clinton."[10] If the United States is so vulnerable, cynics argue, then why have Iraq or Osama bin Laden not succeeded in an information attack? However, typical citizens intimidated by computers and troubled by Windows lockups may be inclined to believe the worst.

The Law of the Computer

IW law has not followed the custom of other mediums. Domestic, not international, law was the original focus since the United States held an early monopoly on network creation. Due to this, laws protecting network anonymity and privacy are strongly embedded. Consequently, bilateral agreements have emerged as a precursor to unified international law. Some believe current law adequately proscribes hostile computer activity. However, the hope that other nations will accede to US opinion on the matter is without merit. As time will likely erode the present US advantage, the time for agreement is now.

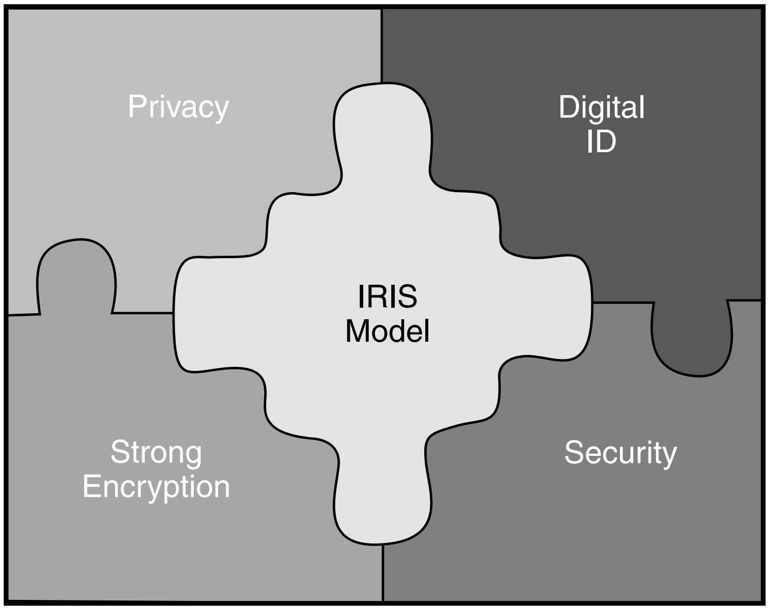
The IRIS Model

The proposed IRIS model mirrors space sanctuary by admitting unrestricted weapons development. Acknowledging this, the model prohibits the deployment, not the development, of computer attack weapons. The IRIS regime treats illicit computer intrusion as a universally criminal act. State-sponsored computer intrusion is defined as an act of aggression, and CNA is a use of armed force. While space sanctuary is the borrowed model, the advantages resemble those of maritime law.

The advantages associated with implementing the IRIS model accrue due to increased security in the peacetime information network and a change in focus for nascent information warriors. Elimination of CNA, as an ideal, protects the global information infrastructure. For the United States, the relative opportunity lost is advantageous since it is the nation most dependent on information systems. The clear communication of rules banning preemptive placement of viruses lessens the risks of brinkmanship and eases cultural anxiety about misinterpretation. Increased security of information provides an added boost to global prosperity. Delineating where IO crosses the boundary from espionage into aggression or use of armed force will simplify the ROE and reduce the time necessary to complete the planning process. Implementation of the IRIS regime can bridge some old gaps while focusing information age competition in the commercial rather than the military sector. However, the myriad of competing agendas necessitates a balanced approach to an IRIS regime implementation.

Feasibility/Trade-Offs

The obstacles to overcome in reaching an IRIS accord are great and would require a succession of sacrifices and trade-offs. As a first requirement, the IRIS regime would have to be verifiable. To be verifiable digital identification of communication would be necessary, but verifying identity would intrude on civil liberties. Universally strong encryption would preserve privacy, but strong encryption would reduce the intelligence-gathering capability of the United States. The ability to verify the source of digital information would decrease intelligence needs and complete this cybernetic circle of life. Most importantly, the strengthening of US communications security and the overall decreased risk of conflict due to global prosperity would decrease the need for intelligence. See figure 13.



Source: Maj Karl J. Shawhan

Figure 13. Trade-Offs

Civil Liberties

Technologies for digital identification exist but are not in widespread use due to the passion for privacy on the Internet. Intel Corporation's recent debut of the Pentium III processor with embedded identification received a lot of bad press. Immediately panned for enabling "big brother's oversight," Intel quickly released a utility that would disable the feature. "The controversial part of the processor serial number is the fact that, when enabled, your unique ID could serve as a unique tracking identifier for you and your computer while on the Internet. Theoretically the processor serial number is intended to only offer a method of informing users of the rated clock speed of their processor while also allowing for greater security during on-line transactions since your unique ID can only be assigned to a single processor, and therefore a single computer, yours."[11] Intel boasts that the processor serial number will "enhance system and asset tracking" by information technology managers.[12] Security with the chip is not perfect since the chip cannot report who is at the computer. However, an enhanced network including this innovation will go a long way towards improving cyberforensics and oversight. Civil libertarians should not confuse anonymity with privacy. The telephone, with caller identification, is not anonymous. Privacy is the only legitimate commodity anonymity protects in a weak encryption construct. If civil libertarians could be assured of privacy through encryption, then their opposition to digital identification would be without merit. Strangely enough, one path to strong encryption runs through a hardware-encoded serial number. Kim Schmitz, chief executive officer of Data Protect GmbH confirms, "A cryptographically secure implementation would use the serial number as the key to a sufficiently strong hard-wired crypto-algorithm."[13] The difficulty lies in getting civil libertarians and intelligence in the same camp.

Intelligence Needs

Universally strong encryption would satisfy privacy needs but leave the intelligence business scrambling. Anyone who has updated his encryption software to 128-bit security through Microsoft or Netscape has had to validate his residence in the United States. This is due to US export controls on encryption technology. This allows supercomputers used by US intelligence organizations to decrypt international communications. If information is the currency of intelligence, then decryption is a mint that keeps issuing. To maintain this power, intelligence agencies of the West have colluded to prevent the use of strong encryption in international communications.

> Last December, bureaucrats from the Department of Foreign Affairs and Trade, advised by the Department of Defense, signed a broad-ranging ban on mass-market cryptography, effectively globalising elements of United States anti-cryptography policy.
>
> The Wassenaar Arrangement, backed by 33 governments around the world including the US, Japan, Canada and many European countries, was condemned by computer freedom activists such as Electronic Frontiers Australia and its US sister group, the Electronic Frontiers Foundation.[14]

In the debate of quality versus quantity, the intelligence corps might be convinced to trade encryption for digital identification. Digital identification would simplify locating the origin of a cybercriminal, which is presently difficult. In the end the intelligence services will be trading something they are about to lose anyhow. The international agreement to limit encryption is unsupportable. According to Professor Henry Beker, president of the United Kingdom's Institute of Mathematics and Its Applications, the agreement has little impact because many signatory countries will simply ignore it. "You'll find that countries like Germany that always stick to the letter of these things may stick to this, but a lot of other countries, like Italy and Spain, will just ignore it when they need to and electronic commerce will just continue on."[15] An American firm, RSA Data

Security Incorporated, has already succeeded in circumventing the export controls. “RSA, which last year turned a $50m profit, has adroitly sidestepped that ban by opening a branch in Australia, a nation with more flexible encryption export regulations. The move gives RSA Data Security Australia access to a global market for encryption technology. In the few weeks it has been operating, Bidzos claims, the new Brisbane-based operation has ‘already done business worth millions.’”[16] In another blow to encryption limits, due for appeal, the US Ninth Circuit Court of Appeals on 6 May 1999 “ruled unconstitutional the U.S. government’s ban on exporting source code for strong encryption.”[17] Intelligence services should rejoice that within IRIS they are getting something for relatively nothing.

Strong encryption will diminish the United States’s ability to peer into international communications. However, recent intelligence deficiencies demonstrate that decryption is no panacea. In spite of encryption limits, the United States missed India’s preparation for a nuclear detonation. Decryption has not revealed how to topple Saddam Hussein or delegitimize Slobodan Milosevic. The presence of decryption does not deter human espionage, which was recently highlighted at nuclear weapons laboratories. In retrospect a change in focus from digital to human sources may actually benefit the intelligence community.

Internet2—A Vehicle for Change

The entrenched interests opposed to an IRIS regime could be moved by the impetus of a future Internet. Internet2 and the Next Generation Internet (NGI) are experimental programs demonstrating capabilities 100 to 1,000 times faster than the present Internet.[18] Designed to meet the large bandwidth needs of universities and laboratories, the programs are harbingers to a future universal Internet. As telegraph users eagerly converted to the telephone, the new Internet will make the old one a nostalgic memory.

Currently in the planning stage, the security requirements for Internet 2 and NGI could incorporate IRIS architecture. Mandatory digital identification would add little to the cost of an Internet2 capable system since new hardware is already necessary to take advantage of the extreme speeds. As with any emerging technology, the system could be backward-compatible with older computers. Large investments in infrastructure such as fiber optics are necessary to deliver these speeds to the home. Initially, only Internet fanatics or the wealthy will invest in the upgrades. Subsequently, as the new web becomes prevalent, a greater portion of the total system will be secure. A grace period would permit a reasonable amount of time before all systems are converted. Upon expiration of the grace period, the old Internet needs to be severed from the new to prevent corruption. This outmoded system could harbor those who value anonymity over security, while the leftover intelligence decryption branch keeps an eye on them.

Reap What You Sow

The world is in the midst of an information revolution, with disparate visions of the revolution's outcome. Indeed, there are many barriers to international accord on IO. However, the journey is not unworthy just because the task is onerous. To coin a phrase, the United States can lead, follow, or get in the way. If it chooses to interfere, the United States can object to changes in the status quo—seemingly with its head in the sand. To follow, it can permit other nations to control the issues that surround the future of digital communication and acquiesce. As a leader, however, the United States can chart a bold future of confidence and security. Regarding arms control, Reagan once said, "Trust, but verify." A future within an IRIS regime captures this spirit of faith. There are no guarantees that other nations will consent to a US position on IW. Consequently, requirements for an IRIS compliant system can exist within emerging technology protocols. The NGI or Internet2 provide the vehicle for change.

The United States stands as the most successful democratic republic. Allowing strong encryption will tell the world that what is good enough for US citizens is good enough for all. It would end the irony of a nation that cherishes liberty while keeping tabs on international communication. The IRIS regime would demonstrate that after the cold war, the United States can focus on winning the next war and still lead the charge for democracy. Indeed, from the 1997 *NMS:* "Engagement activities, including information sharing and contacts between our military and the armed forces of other nations, promote trust and confidence and encourage measures that increase our security and that of our allies, partners, and friends. By increasing understanding and reducing uncertainty, engagement builds constructive security relationships, helps to promote the development of democratic institutions, and helps keep some countries from becoming adversaries tomorrow."[19] An IRIS regime would fortify the primary national security strategy objectives to *enhance US security, bolster America's economic prosperity, and promote democracy abroad*. For the United States, the IRIS regime's embedded virtues of liberty are a superior vehicle for a strategy of engagement.

Notes

1. John D. Jones and Marc F. Griesbach, eds., *Just War Theory in the Nuclear Age* (Lanham, Md.: University Press of America, 1985), 3–34.

2. Charles A. Roberts, "Outer Space and National Sovereignty," *Air University Quarterly Review* XII, no. 1 (Spring 1960): 55–56.

3. Martin B. Schofield, "Control of Outer Space," *Air University Quarterly Review* X, no. 1 (Spring 1958): 93.

4. Roberts, 54.

5. Walter A. McDougall, *The Heavens and the Earth: A Political History of the Space Age* (Baltimore: Johns Hopkins University Press), 415–35.

6. Bruce M. DeBlois, “Space Sanctuary: A Viable National Strategy,” *Airpower Journal* XII, no. 4 (Winter 1998): 41–57.

7. *A National Security Strategy for a New Century* (Washington, D.C.: White House, May 1997), i.

8. Ibid., 5.

9. Ibid.

10. George Smith, “An Electronic Pearl Harbor? Not Likely,” *Issues in Science and Technology*, Fall 1998, 68–73.

11. Anand Lai Shimpi, “Intel Pentium III,” *Anand Tech*, 22 February 1999, n.p.; on-line, Internet, 28 March 1999, available from http://www.anandtech.com/html/review_display.cfm?document=902.

12. “Pentium III Processor: Business Benefits—The No-Compromise Solution for Business Computing,” *Intel Corporation*, n.p.; on-line, Internet, 28 March 1999, available from http://www.intel.com/businesscomputing/pentiumiii/.

13. Tom Pabst, “Is Intel’s New CPU Identification for Data Security Only a Marketing Gag?” *Tom’s Hardware Guide*, 21 January 1999, n.p.; on-line, Internet, available from http://www.tomshardware.com/releases/99q1/9901211/index-01.html.

14. John Davidson, “Australia: Cryptography Cyber Treaty Will Have No Effect—Expert,” *InfoWar*, 19 January 1999, n.p.; on-line, Internet, 28 March 1999, available from http://www.infowar.com/class_1/99/class1_020399b_j.shtml.

15. Ibid.

16. Tim Blair, “Online and Out of Reach: The Privacy War between Software Geeks and FBI Spooks Moves to a New Battleground: Australia,” *Time*, 1 February 1999, n.p.; on-line, Internet, 15 December 2000, available from http://www.time.com/time/magazine/article/0,9171,20427,00.html.

17. Elinor Mills, “Court Dumps Code Export Ban,” *PC World News*, n.p.; on-line, Internet, 7 March 1999, available from http://www.pcworld.com/pcwtoday/article/0.1510,10857,00.html

18. “Internet2 and the NGI: Complementary and Interdependent,” *Internet2*, n.p.; on-line, Internet, 28 March 1999, available from http://www.internet2.edu/html/internet2-ngi.html.

19. 1997 *NSS*, Preface; and, *A National Security Strategy for a New Century*, October 1998, Preface.